NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EMBRACING THE DEVIL: AN ANALYSIS OF THE FORMAL ADOPTION OF RED TEAMING IN THE SECURITY PLANNING FOR MAJOR EVENTS

by

Thomas Owen Landry

March 2017

Thesis Co-Advisors: Carolyn Halladay
Christopher Bellavita

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2017	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE EMBRACING THE DEVIL: AN ANALYSIS OF THE FORMAL ADOPTION OF RED TEAMING IN THE SECURITY PLANNING FOR MAJOR EVENTS			**5. FUNDING NUMBERS**
6. AUTHOR(S) Thomas Owen Landry			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The Department of Homeland Security (DHS) takes the lead or a significant supporting security role in many of the nation's most celebrated events across the country. Major events that receive the official designation of a national special security event and those rated Level 1 on the DHS special event rating scale share the same subcommittee planning structure. This thesis focuses on the potential vulnerabilities and gaps in the planning process due to groupthink and other organizational and individual decision-making pitfalls. This thesis then reviews what, if any, potential improvements can be made to the process with the formal adoption of a red team component.

This thesis examines the potential benefits of incorporating red team techniques, such as simulation exercises, vulnerability probes, and analytical analysis into major-event security planning. Research indicates that their effectiveness varied on the organizational leadership, team composition, and independence afforded these teams in the performance of their assignment. The process of red teaming is vulnerable to being marginalized without proper organizational support. Armed with this knowledge, this thesis proposes two recommendations for the formal adoption of red team techniques into the subcommittee process of major-event security planning.

14. SUBJECT TERMS Department of Homeland Security, red team, groupthink, major event security, United States Secret Service			**15. NUMBER OF PAGES** 83
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

EMBRACING THE DEVIL: AN ANALYSIS OF THE FORMAL ADOPTION OF RED TEAMING IN THE SECURITY PLANNING FOR MAJOR EVENTS

Thomas Owen Landry
Deputy Special Agent in Charge, United States Secret Service
B.A., Miami University, 1996
M.A., Northeastern University, 1997

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2017**

Approved by: Carolyn Halladay
Thesis Co-Advisor

Christopher Bellavita
Thesis Co-Advisor

Erik Dahl
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Department of Homeland Security (DHS) takes the lead or a significant supporting security role in many of the nation's most celebrated events across the country. Major events that receive the official designation of a national special security event and those rated Level 1 on the DHS special event rating scale share the same subcommittee planning structure. This thesis focuses on the potential vulnerabilities and gaps in the planning process due to groupthink and other organizational and individual decision-making pitfalls. This thesis then reviews what, if any, potential improvements can be made to the process with the formal adoption of a red team component.

This thesis examines the potential benefits of incorporating red team techniques, such as simulation exercises, vulnerability probes, and analytical analysis into major-event security planning. Research indicates that their effectiveness varied on the organizational leadership, team composition, and independence afforded these teams in the performance of their assignment. The process of red teaming is vulnerable to being marginalized without proper organizational support. Armed with this knowledge, this thesis proposes two recommendations for the formal adoption of red team techniques into the subcommittee process of major-event security planning.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CAS	Civil Aviation Security
CBP	Customs and Border Patrol
CIA	Central Intelligence Agency
DHS	Department of Homeland Security
DOD	Department of Defense
ESC	Executive Steering Committee
FAA	Federal Aviation Authority
FEMA	Federal Emergency Management Agency
FOIA	Freedom of Information Act
FOUO	For Official Use Only
HSPD	Homeland Security Presidential Directive
IC	intelligence community
IED	improvised explosive device
JCCIC	Joint Congressional Committee on Inaugural Ceremonies
JFCOM	Joint Forces Command
MC	Millennium Challenge
MERT	Major Event Red Team
NFL	National Football League
NORAD	North American Aerospace Defense Command
NPPD	National Protection and Programs Directorate
NSSE	national special security event
OE	operational environment
PDD	Presidential Decision Directive
SEAR	special event activity rating
SEWG	Special Event Working Group
UAV	unmanned aerial vehicle
UFMCS	University of Foreign Military and Cultural Studies
USCP	U.S. Capitol Police
USSS	United States Secret Service
WMATA	Washington Metropolitan Area Transit Authority

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The Department of Homeland Security (DHS) takes the lead or a significant supporting security role in many of the nation's largest and most celebrated events across the country. These political, sporting, and cultural events present the nation's adversaries with inviting targets due to the size, scope, and historical significance of the occasions. Often these events are attended by senior governmental leaders from the United States, as well as foreign countries. Group decision-making errors, assumptions in the planning process, and the failure to anticipate an ever-changing enemy or conditions can leave major events vulnerable to attack or serious disruption. Security planners must consider not only purposeful physical attacks, but also the whole spectrum of environmental, fire and life safety, and civil disobedience when designing countermeasures to risk.

This thesis analyzes the planning process used to design and implement security procedures for major events throughout the country. Specifically, it examines security planning for events designated as a national special security event or those that receive a special event activity rating Level 1 from the DHS. This thesis focuses on the potential vulnerabilities and gaps in the planning process due to groupthink and other organizational decision-making pitfalls. The subcommittee process employed in these major events has proven effective in marshaling tremendous amounts of resources and ensuring that areas of responsibility are well-defined; however, it leaves open the potential for individual and organizational biases to impact planning. This project has explored the varieties of red team techniques available to major event security planners and asked the question: *How would the Department of Homeland Security (DHS) benefit from formally adopting a red team component to major-event security planning?* This thesis then reviews which, if any, potential improvements can be made to the process with the formal adoption of a red team component. This paper derives data and evidence exclusively from publically available academic literature and after-action reports. It features a case study of the 2009 presidential inauguration, drawn from comparable publically released material. This project uses a blend of policy analysis and the

case study method during the course of this project. The case study method relies heavily on the results of a small group of events that may be vulnerable to sampling bias and lead to results that may not be easily generalizable.

The concepts and techniques of red teaming are being taught and increasingly used and accepted throughout the United States within the Department of Defense and the intelligence and law enforcement communities. The potential benefits and drawbacks of simulations, vulnerability probes, and analytical techniques have been explored in this project. While not all red team techniques are ideally suited for use in major event security design, the expanded use of analytical analysis has the potential to challenge organizational thought and assumptions. These techniques, however, need to be completed within the subcommittee framework used in the design and execution of security for major events.

Based on the findings on red team performance and execution pitfalls, this thesis has made two proposals to insert formally an analytical red team capability into the framework used in major-event security planning. The proposals have the potential to place properly trained individuals into the framework at the appropriate time to make improvements into the planning process. These proposals, however, must navigate the minefield of potential execution errors outlined in this thesis. While the DHS may theoretically benefit from the formal adoption of analytical red team techniques, the execution limitations discussed in this thesis reduce the likelihood for ideal results. The DHS needs to consider these limitations before formally adopting a red team component into the framework for major-event security planning.

ACKNOWLEDGMENTS

I would like to take this opportunity to thank some of the many individuals who made this opportunity possible. This list begins with my outstanding and supportive committee, Dr. Carolyn Halladay and Dr. Christopher Bellavita, of the Naval Postgraduate School. They patiently demonstrated to me that “assumptions” are bad not only in security planning, but also in academic research. Their persistence and direction have been invaluable and they have my sincere gratitude.

To Cohort 1511, I am grateful to have shared this journey with you. Each of you brought a unique experience, knowledge, and personality to the collective table and made this program even more rewarding. I wish you all the best in your future careers, and I look forward to watching your contributions to the homeland security mission.

My professional colleagues at the United States Secret Service, George W. Bush Protective Division, deserve special thanks. Specifically, Special Agent in Charge Paul H. Maurer, for supporting me in this program and for picking up my workload as I attended the quarterly in-residence periods.

Most importantly, my love and appreciation goes to my family who sacrificed in countless ways to enable me to complete this program. My wife, Dr. Suja Nair, son (Rajiv Leo), and daughter (Jaya Isabella), have been amazingly supportive in this endeavor and are a blessing to me every single day. There remains nothing we cannot do together. To my departed father, Leo Joseph Landry, who demonstrated to me daily the power of consistency and perseverance. Despite barely graduating from high school, he remains the wisest man I have ever met and surely would have appreciated that I never let my schoolwork get in the way of my education.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

We can be blind to the obvious, and we are also blind to our blindness.[1]

~ Daniel Kahneman

The Department of Homeland Security (DHS) takes the lead or a significant supporting security role in many of the nation's largest and most celebrated events across the country. Examples of such events include presidential inauguration ceremonies, major political conventions, State of the Union events, world leader summits, such as the annual United Nations General Assembly, and the National Football League (NFL) Super Bowl. These political, sporting, and cultural events present the nation's adversaries with inviting targets due to the size, scope, and historical significance of the occasions. Each year, these events draw hundreds of thousands of attendees and they are watched on television and social media by millions of viewers across the country and around the world. Often, these events are attended by senior governmental leaders from the United States, as well as foreign countries. An example can be seen in the 2012 NATO Summit held in Chicago, Illinois where senior diplomats and heads of state from all 28 member nations were in attendance.

Securing the nation's most significant events requires the participation of the entire homeland security enterprise. Local, state, and federal agencies come together to design and execute security plans under significant resource and often planning timeline constraints.[2] Currently, a subcommittee process of coordination is employed for these events and this approach has positive and negative attributes. Small groups of homeland security leaders determine the threats and vulnerabilities that will receive the most resources and countermeasures in the design and implementation of security plans.

---

[1] Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus, and Giroux, 2011), 24.

[2] Planning timelines vary by the type of event and can range from years (2002 Olympic Games in Salt Lake City, Utah) to days (U.S. Presidential funerals, such as the 2006 funeral of Former President Gerald Ford).

Group decision-making errors, assumptions in the planning process, and the failure to anticipate an ever-changing enemy or conditions can leave major events vulnerable to attack or serious disruption. Security planners must consider not only purposeful physical attacks, but also the whole spectrum of environmental, fire, and life safety, and civil disobedience when designing countermeasures to risk. At worst, a real or perceived significant security failure in these events could lead to the destabilization of the U.S. government, as well as negatively impacting world geo-politics. Financial markets around the world can also be jeopardized in the short-term with trillions of dollars of wealth at risk in the aftermath of a major security incident. As an example, the New York Stock Exchange lost more than seven percent in value in the first day of stock trading after the terror attacks of 9/11.[3] At the very least, poor operational planning by security managers will quietly lead to the waste of millions of dollars of tax payer funds in designing and executing plans ill-suited for the risks of today and in no way preparing for the enemy of tomorrow. In an effort to avoid these worst-case scenarios this thesis asks: *How would the Department of Homeland Security (DHS) benefit from formally adopting an analytical red team component into the subcommittee process for major-event security planning?*

This thesis analyzes the planning process used to design and implement security procedures for major events throughout the country. Specifically, it examines security planning for events designated as a national special security event (NSSE) or those that receive a special event activity rating (SEAR) Level 1 from the DHS. Special events that fall below these ratings often do not require the same level of multi-agency coordination and do not use the same organizational framework as NSSE and SEAR Level 1 events.[4] NSSE and SEAR Level 1 events use a subcommittee design that makes the decision-making process unique. Events that receive a lower SEAR typically do not use the subcommittee process and are not subject to the same planning process issues. The

[3] Mark Davis, "How 9/11 Affected the U.S. Stock Market," Investopedia, September 9, 2011, http://www.investopedia.com/financial-edge/0911/how-september-11-affected-the-u.s.-stock-market.aspx. Stock market losses did rebound within one month; however, the short-term risk to the financial markets was demonstrated.

[4] This rating does not mean that these events are at any less risk from attack or disruption, just that the planning process is different and outside the scope of this paper.

processes by which events are rated by the DHS, as well as the subcommittee planning process, are discussed in Chapter III.

This thesis focuses on the potential vulnerabilities and gaps in the planning process due to groupthink and other organizational decision-making pitfalls. It then reviews which, if any, potential improvements can be made to the process with the formal adoption of a red team component. Would the formal adoption of red teaming into the planning process reduce individual biases and reduce organizational blindness? Would potential incidents of groupthink be reduced by the aggressive use of a red team component or the adoption of formal techniques, such as the "devil's advocate"? If the answer is yes, determining exactly "who" should complete this analysis is just as important as "if" it should be done at all. Additionally, this thesis reviews currently used red teams to determine potential pitfalls and limitations in the execution of these techniques. The results of this analysis indicate that the subcommittee process used in major event security is vulnerable to group decision-making errors; typically, security experts recommend red teams. In this particular context, however, formally adopting analytical red teams may not offer a failsafe solution.

A. LITERATURE REVIEW

Literature on groupthink and other common decision-making pitfalls is widely available. Documentation on the role of groupthink specifically in the security planning for major events, however, is virtually non-existent. Potential reasons for this lack of academic literature may include the perceived necessity of governmental organizations to maintain operational security in the planning process, as well as the lack of a significant catastrophic occurrence involving a major security event.

1. Groupthink and Other Decision-Making Traps

Although the basic concept of groupthink was outlined in the 1952 *Fortune Magazine* article entitled "Groupthink" authored by William H. Whyte Jr., it was not until 1972 that the groundbreaking research of Yale University psychologist Irving L. Janis propelled the theory into the mainstream of psychology. The publication of Janis's

original work, *Victims of Groupthink*, in 1972 was followed up a decade later by his expanded version, *Groupthink: Psychological Studies of Policy Decisions and Fiascos*.

Janis defined groupthink as "a deterioration of mental efficiency, reality testing, and moral judgment that results from in-group pressures."[5] Janis began his work by outlining the "imperfect" connection between groupthink and decision-making disasters. No direct correlation exists between poor outcomes and defective decision making.[6] Pure luck, adversarial incompetence, and "lucky accidents" often lead to good outcomes in decisions, but these flashes should not be confused with actual high functioning teams. This concept is especially important when considering the security preparations for major events, as a lack of an incident should not be construed as evidence of outstanding or effective planning.

Through his academic work on group decision making, Janis identified several conditions often present in groupthink, symptoms of the phenomenon, and the consequences of defective decision making. Janis also outlined the significant symptoms and organizational structures frequently present in occurrences of groupthink. He reviewed case studies of some of modern histories largest "fiascos" to include Pearl Harbor, the Bay of Pigs invasion, and the escalation of the Korean and Vietnam wars. From these case studies, Janis identified the following eight symptoms most often associated with groupthink: illusion of invulnerability, the belief in the group's inherent morality, collective rationalization that inhibits consideration of new ideas, stereotyped views of the enemy, self-censorship, shared sense of unanimity, direct pressure against those members who do not share the group consensus, and lastly, the emergence of self-appointed "mindguards."[7] Mindguards are described by Janis as "group members who protect the group from adverse information that might shatter their shared complacency

---

[5] Irving Janis, *Groupthink: Psychological Studies of Policy Decisions and Fiascos* (Boston: Houston Mifflin Company, 1982), 9. This book is a revised and enlarged version of his original 1972 work entitled *Victims of Groupthink: Psychological Studies of Foreign-Policy Decisions and Fiascos*.

[6] Ibid., 11.

[7] Ibid., 174–175.

about the effectiveness and morality of their decisions."[8] These symptoms do not exist in every situation and often they exist in varying degrees.

Conditions often present in cases of groupthink, referred to by Janis as "antecedent," can be structural or psychological in nature. Structural conditions to groupthink include a high-level of insulation of the group, the lack of impartial leadership, lack of decision-making norms, and homogeneity of group membership.[9] Psychological conditions for groupthink include high stress from external threats with little hope of a better solution, low self-esteem temporarily induced by recent failures, and difficulties in determining feasible alternatives in decisions involving moral dilemmas.[10]

The organizational structure within which a group operates also has an impact on the occurrence of groupthink and decision-making performance. Janis identified four organizational structural antecedent conditions present in many cases of groupthink: insulation of the group, lack of impartial leadership, lack of a normative decision process, and group homogeneity.[11]

These four structural antecedent conditions discussed by Janis were elaborated on in James Ricciuti's 2014 master's thesis: "Groupthink: A Significant Threat to the Homeland Security of the United States." Ricciuti's work identified evidence of groupthink in several DHS component agencies to include the United Stated Secret Service and the Federal Air Marshal's Service.[12]

Janis's case study research focused on observable consequences of groupthink in political situations. The more symptoms of groupthink exhibited, the more likely that

---

[8] Ibid., 175.

[9] Janis, *Groupthink: Psychological Studies of Policy Decisions and Fiascos*, 244.

[10] Ibid.

[11] Ibid.

[12] James E. Ricciuti, "Groupthink: A Significant Threat to the Homeland Security of the United States" (master's thesis, Naval Postgraduate School, 2014), 46–51.

defective decision making will occur in the group setting.[13] Janis focused on the following seven observable consequences of defective decision making:

- incomplete survey of alternatives
- incomplete survey of objectives
- failure to examine risks of preferred choice
- failure to reappraise initially rejected alternatives
- poor information search
- selective bias in processing information at hand
- failure to work out contingency plans[14]

Individual decision-making errors are actually made worse in groups in many cases according to Cass Sunstein and Reid Hastie's book, *Wiser: Getting Beyond Groupthink to Make Groups Smarter.* Many individual decision-making issues, such as the availability and representative heuristics, egocentric bias, and the sunk cost fallacy, are all amplified in the group setting.[15] Additionally, Sunstein and Hastie proposed that the concept of group polarization increases in groups for three principle reasons: informational influence, social pressures, and group confidence. Informational influences refer to the concept that individuals have a natural tendency to follow arguments that mirror their own.[16] Group confidence is used by Sunstein and Hastie to mean that individuals who agree with one another have a tendency to push the group to the more extreme position.[17] Like-minded individuals can "convince" themselves of the validity of their collective thoughts by simply reinforcing it within the group. The chances of group polarization can also be increased when the members of the group have a shared identity.[18] In-group and out-group identities can work to strengthen feelings of group

[13] Janis, *Groupthink: Psychological Studies of Policy Decisions and Fiascos,* 175.

[14] Janis, *Groupthink: Psychological Studies of Policy Decisions and Fiascos,* 175, 244.

[15] Cass Sunstein and Reid Hastie, *Wiser: Getting Beyond Groupthink to Make Groups Smarter* (Boston: Harvard Business Review Press, 2015), 44–51.

[16] Ibid., 83.

[17] Ibid., 84–85.

[18] Ibid., 85.

polarization in decision making. The law enforcement profession can drive strong feelings of social identity that can feed into potential group polarization.[19]

Not only can groups impact decision-making capabilities, but the actual organizational framework can have a negative impact on decision making and planning. Gillian Tett, a cultural anthropologist, focused on the sub-divisions that exist within large organizations and the lack of communication between these sub-groups in her 2015 book, *The Silo Effect*. This book focused on eight different case studies involving both government agencies and private industries to examine how groups interact with one another and the gaps that can develop between "silos of experts" within the same organization. Tett proposed that specialized groups of subject matter experts are a positive development in the modern world, but can lead to planning errors and poor information exchange.[20] "Fragmentation can create information bottlenecks and stifle innovation. Above all else, silos can create tunnel vision or mental blindness, which causes people to do stupid things," according to Tett.[21] These "silos" resemble the subcommittee framework used in the design and execution of major event security discussed in Chapter III.

Gary Klein's book, *Seeing What Others Don't*, outlines several ways in which organizational bureaucracy can impede insights and inspired solutions. The "predictability trap" occurs when team members bring creative ideas to management; however, the agency resists these ideas because they inherently will change the preexisting operational plan. This resistance comes from a desire to maintain as much predictability as possible, as insights and creative ideas bring instability and potentially unknown outcomes. Some organizations intrinsically place a premium on the reduction of errors and uncertainty that can get in the way of creative decision making.[22] This focus on the reduction of errors can lead to agencies attempting simply to dust off the old

---

[19] M. Brent Hood, "Us versus Them: Effects of Group Dynamics on Leadership," FBI Law Enforcement Bulletin, June 2015, https://leb.fbi.gov/2015/june/us-versus-them-effects-of-group-dynamics-on-leadership.

[20] Tet Gillian, *The Silo Effect* (New York: Simon and Schuster, 2015), 13–14.

[21] Ibid., 14.

[22] Gary Klein, *Seeing What Others Don't* (New York: Public Affairs Press, 2013), 157.

playbook from the last event and update it to fit the current scenario. This concept was described as "methodism" by Carl von Clausewitz, as discussed by Dietrich Dorner in his book, *The Logic of Failure*. Dorner went on to explain that "psychological experiments have demonstrated how people's range of actions is limited by their tendency to act in accordance with pre-established patterns."[23]

Even potentially more insidious is the subtle individual bias that may exist against creativity. The *Psychological Science* article, "The Bias Against Creativity: Why People Desire But Reject Creative Ideas?," written by Jennifer Mueller and associates, detailed two studies to measure participant's *implicit*, as well as *explicit* attitudes toward creativity relative to practicality in controlled experiments. Study results indicated that when participants were given an immediate goal of reducing uncertainty, it led to lower ratings of the perceived creativity of words, which occurred despite the participants demonstrating a positive *explicit* association towards creativity. The second experiment demonstrated that introducing an element of uncertainty into the process promoted a "negative association with creativity relative to practicality and extended this finding by showing that bias against creativity interfered with participants' ability to recognize a creative idea."[24] As much as individuals expressed a desire to embrace creative solutions, participants in this test consistently chose practicality and predictability.

The desire for predictability was so strong in corporate America that it led to the design and implementation of the *Six Sigma* program in the late 1980s. This program was designed by Motorola as a way to reduce errors and improve the quality of their products.[25] *Six Sigma* was initially extremely successful in reducing production errors and costs, but at the expense of innovation in the long term.[26]

Klein also focused on what he referred to as the "perfection trap" in *Seeing What Others Don't*. Perfection in this context means an organizational desire to execute the

---

[23] Dietrich Dorner, *The Logic of Failure* (New York: Metropolitan Book, 1996), 45.

[24] Jennifer S. Mueller, Shimul Melwani, and Jack A. Goncalo, "The Bias Against Creativity: Why People Desire but Reject Creative Ideas," *Psychological Science* 23, no. 1 (2012): 16.

[25] Klein, *Seeing What Others Don't*, 222.

[26] Ibid., 223.

plan exactly as was initially designed.[27] Klein highlighted that for managers, a lot of upside for executing the same plan successfully is involved, as opposed to trying new and creative approaches. The risk involved in attempting new and innovative approaches outweighs the potential creative upside. This "perfection trap" pushes leaders to use old, and potentially no longer appropriate, strategies and methods.

In addition to the conscious decision to resist changes in the design of operational security plans, the theory of *cognitive dissonance* can impact the process in a negative way. Carol Tavris and Elliot Aronson describe cognitive dissonance as "the engine that drives self-justification, the energy that produces the need to justify our actions and decisions-especially the wrong ones" in their 2015 book entitled *Mistakes Were Made (But Not by Me).*[28] This dissonance leads individuals to focus on information that supports their original hypothesis while excluding new information that threatens their position. Tavris and Aronson noted the "backfire effect," in which individuals faced with new information actually increases the support for their original incorrect opinion.[29] Why change the plans for the 2017 State of the Union Address when the plans from 2016 went smoothly?

2. Counterpoints to Groupthink

Several academic studies have attempted to quantify the impact of groupthink and the symptoms outlined by Irving Janis over the last few decades.

Ramon Aldag and Sally Riggs Fuller's article in *The Psychological Bulletin*, "Beyond Fiascos: A Reappraisal of the Groupthink Phenomenon and a New Model of Group Decision Processes" takes a hard look at groupthink. They postulated that groupthink has become popular due more to the "intuitive appeal" than actual empirical

[27] Ibid., 156.

[28] Carol Tavris and Elliot Aronson, *Mistakes Were Made (but Not by Me)* (New York: Houghton Mifflin, 2015), 15.

[29] Ibid., 26. This "backfire effect" is similar to several of the symptoms of groupthink described by Irving Janis.

evidence.[30] The original Janis case studies provided a small sample of qualitative work involving large-scale decisions that calls into question the overall applicability to group decision making. Aldag and Fuller proposed that the groupthink theory needs to be updated incorporating the last few decades worth of research on decision making.[31] While the overall concept of groupthink is called into question with this work, still other studies looked at particular pieces of the groupthink phenomenon.

The impact of leadership style (directional versus participative) and *devil's advocacy*, a red team technique discussed further in Chapter III, in group decision making were studied in the *The Psychological Record*, "Groupthink: Deciding with the Leader and the Devil" by Zenglo Chen and associates in 1996. This study controlled both the leadership style and *devil's advocacy* role in contrast to other empirically based academic studies.[32] Chen et al. ran a study with undergraduate volunteers participating in the "Lost at Sea"[33] survival task with confederates acting as both group leaders and devil's advocates. The empirical results indicated that lower quality decisions were made when the confederate leader demonstrated a directive leadership style (as opposed to participative); however, the devil's advocate produced no appreciable improvements to the results.[34] The authors proposed that the devil's advocate role playing was not strong enough to influence the group decision making. This concept is critical when considering the potential utilization of the devil's advocate in major security planning subcommittees.

---

[30] Ramon Aldag and Sally Riggs Fuller, "Beyond Fiascos: A Reappraisal of the Groupthink Phenomenon and a New Model of Group Decision Processes," *The Psychological Bulletin* 113, no. 3 (1993): 547.

[31] Aldag and Fuller, "Beyond Fiascos," 549.

[32] Zenglo Chen et al., "Groupthink: Deciding with the Leader and Devil," *The Psychological Record* 46, no. 4 (Fall 1996), http://www.thefreelibrary.com/Groupthink%3a+deciding+with+the+leader+and+the+devil.-a018911798.

[33] The Lost at Sea scenario is a team building exercise in which group members must work together to rank order items to be salvaged in a hypothetical boating accident.

[34] Chen et al., "Groupthink."

B. RESEARCH DESIGN

This paper derives data and evidence exclusively from publically available academic literature and after-action reports. It features a case study of the 2009 presidential inauguration, drawn from comparable publically released material.

This thesis uses a blend of policy analysis and the case study method during the course of this project. This method has potential negative aspects that should be considered. This thesis uses official after-action reports that may, or may not, be a complete assessment of the event. Agencies could potentially have their self-interest in mind leading to a less than complete appraisal of major event security performance. Lastly, the case study method relies heavily on the results of a small group of events that may be vulnerable to sampling bias and lead to results that may not be easily generalizable.

This project is broken into six chapters. Chapter II introduces the concept of red teaming and provides the historical origins for these techniques. This chapter also outlines successful uses of red teaming across the government, as well as introduces three different varieties of techniques: simulation exercises, vulnerability probes, and analytical analysis.

Chapter III analyzes the legal framework of responsibilities for local, state, and federal agencies, as well as the official process by which NSSEs and SEAR 1 events are classified, funded, and protected. These responsibilities are derived from presidential order and department regulation. This chapter also reviews the formal organizational structure from several recent major events, such as the 2016 Super Bowl in Santa Clara, CA, the 2012 Democratic National Convention in Charlotte, NC, and the 2012 Republican National Convention in Tampa, FL. Chapter III also introduces the executive subcommittee model used in major event security design and identifies vulnerabilities to the process from both an institutional and individual perspective. This thesis examines the antecedent conditions of groupthink and analyzes the executive subcommittee model used in the security design for NSSEs and SEAR 1 events for potential vulnerability.

Chapter IV, a case study review of the 2009 presidential inauguration, outlines the planning errors that led to crowd management issues. This case study draws material from the declassified after-action report prepared for Congress. This unique document provides a rare look into the subcommittee process for major events including the assumptions made by key members on the planning team.

Chapter V attempts to insert red team techniques into the subcommittee process and proposes how red teaming might have reduced these crowd issues in this major event. This chapter also outlines the critical execution errors and pitfalls that potentially reduce the effectiveness of these techniques in improving decision making. These execution errors are drawn from a review of current red team literature primarily based on Department of Defense (DOD) experiences.

This project proposes a set of policy recommendations for future adoption by the DHS and such component agencies as the United States Secret Service (USSS). Several critical implementation issues are discussed and addressed in this paper as well. Policy recommendations for the inclusion of red teaming in major event security design must consider several of the following critical questions: who exactly completes the red teaming, how will they integrate into the current subcommittee framework, and what results can reasonably be expected from this addition.

C. ANSWERS AND QUESTIONS

This project began with an interest in examining the process by which groups of local, state, and federal homeland security professionals make decisions on how best to secure major events. The impact of groupthink, heuristics, and individual biases play a role in group decision making and homeland security professionals are not immune to their effects. This thesis assumed that the introduction of red team techniques into the subcommittee model of major-event security planning would be a natural improvement to the overall group decision-making process. The research in this project quickly identified that it was not always the case. Theoretically, the techniques outlined in Chapter II may reduce groupthink, improve problem-solving skills, and reduce organizational blindness. In reality, the execution of these techniques present challenges that the researcher did not

anticipate at the beginning of this project. The recommendations contained in this project attempt to account for the difficulties identified in the research for this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

II. RED TEAM TECHNIQUES

> The greatest of faults, I should say, is to be conscious of none.[35]
>
> ~ Thomas Carlyle

This chapter introduces the concept of red teaming and the most common varieties of techniques and how they may improve group decision-making and performance. The DOD and the American intelligence community (IC) have recognized potential pitfalls in their planning and analytical operations and embraced the concept of red teaming across their organizations. This same concept may improve the security planning operations for major security events by reducing groupthink and challenging organizational assumptions.

A. HISTORICAL ORIGINS OF RED TEAM TECHNIQUES

Pope Gregory IX, in an attempt to formalize and exert greater control over the canonization process in the Roman Catholic Church, established the *Advocatus Diaboli* in 1234.[36] The *Advocatus Diaboli*, or Devil's Advocate, was tasked as the "designated dissenter" and was responsible for providing objections and counter-evidence against all individuals nominated for sainthood.[37] This new process inadvertently gave birth to the concept of red teaming, demonstrating the potential role for contrarian thought in organizations. Pope John Paul II discarded the devil's advocate when he streamlined the canonization process in 1983.[38] Perhaps incidentally, Pope John Paul II also presided over more beatifications and canonizations in the next 20 years than had occurred over the preceding 2,000 years.[39] It is difficult to determine the effectiveness of the *Advocatus Diaboli* in the canonization process for the Roman Catholic Church, but the removal of

[35] Tarvis and Aronson, *Mistakes Were Made*, 58.

[36] Micah Zenko, *Red Team: How to Succeed by Thinking Like the Enemy* (New York: Basic Books, 2015), XI.

[37] Ibid.

[38] Ibid.

[39] Ibid.

the designated dissenter lead to a sharp increase in those granted this rare declaration from the church.

Although red team techniques have been used historically in the American military under various names, the very term "red team" originated from the DOD during the Cold War in the 1960s.[40] The DOD's use of red teams and techniques was sporadic and inconsistent across the armed services until the 2003 Defense Science Board task force report titled *The Role and Status of DOD Red Teaming Activities.*[41] This report was completed in the aftermath of the events of 9/11 and sought to review current red team best practices to determine if these techniques should be put to greater use in the department.[42] This task force made the formal recommendation that the Secretary of Defense "take steps to inculcate effective red team use throughout the department" to identify weaknesses before real adversaries do.

The largest single source of red team training in the United States is the U.S. Army's University of Foreign Military and Cultural Studies (UFMCS) located in Fort Leavenworth, Kansas. The UFMCS was formed in 2004 and tasked with changing the way the military thinks, including countering the effects of groupthink in the formal command structure.[43] Although technically an Army facility, this course is attended by members of all branches of the military. The U.S. Army awards the red team certification to individuals who successfully pass the UFMCS course. Army commanders may then call on these officers as needed to provide an alternative perspective or to challenge the assumptions in planning.[44] This technique provides Army leadership with a maximum

---

[40] Zenko, *Red Team: How to Succeed by Thinking Like the Enemy*, 26. The "red" referred to the United States' largest adversary at the time: the Soviet Union.

[41] Ibid., 28.

[42] Defense Science Board, *The Role and Status of DoD Red Teaming Activities* (Washington, DC: Office of the Under Secretary of Defense, 2003), 1.

[43] Zenko, *Red Team: How to Succeed by Thinking Like the Enemy*, 38. The United States Marine Corps also began red team instruction in this same timeframe as part of the Marine Corps University in Quantico, Virginia.

[44] Ibid., 39.

amount of flexibility without having the expense of having to support a standalone full-time red team.[45]

This program has produced a publically available 240-page manual titled the *Applied Critical Thinking Handbook*, which is, in essence, a formal training manual in the discipline of red team techniques used throughout the military.[46] In addition to the *Applied Thinking Handbook*, the UFMCS has published the *UFMCS Group Think Mitigation Guide* in 2014. This guide outlines several current strategies to minimize the impact of groupthink on operations and used to teach new military officers techniques to recognize biases in their thought process.[47] Specifically, the handbook advances four major tenets designed to improve an individual's ability to make decisions in constantly changing environments: fostering cultural empathy, self-reflection and awareness, groupthink mitigation, and applied critical thinking.[48]

Although the demand for the courses taught at the UFMCS have been growing since inception, no formal measurement of how effective the skills taught there have been in improving overall DOD planning and reducing decision-making errors has been done.[49]

B. THE CONCEPTS AND TECHNIQUES OF RED TEAMING

Depending on the sector, business, government, the IC, or the military, red teaming may occur under a variety of names and with different goals. Mark Mateski, founder and editor of *The Red Team Journal*, states the goal of the modern red team is "to enhance decision making by challenging assumptions and exploring new ideas, typically

---

[45] Zenko, *Red Team: How to Succeed by Thinking Like the Enemy*, 39.

[46] Ibid.

[47] Both of these guides are available online to the general public.

[48] University of Foreign Military and Cultural Studies, *The Applied Critical Thinking Handbook (formerly the Red Team Handbook)*, ver. 8.1 (Fort Leavenworth, KS: University of Foreign Military and Cultural Studies, 2016), 4–7.

[49] Zenko, *Red Team: How to Succeed by Thinking Like the Enemy*, 40.

from the perspective of an adversary or a competitor."[50] The UFMCS uses the following definition:

> Red teaming is a function that provides commanders an independent capability to fully explore alternatives in plans, operations, concepts, organizations and capabilities in the context of the operational environment (OE) and from the perspectives of partners, adversaries and others.[51]

According to the UFMCS, DOD red team practitioners complete three general types of tasks:

- decision support to operations, planning, and decision making
- critically review and analyze existing plans
- emulate enemy behavior and testing[52]

Red teaming is not an exact science and the appropriate technique used will depend on the individual scenario in question. While attempting to complete the previously listed tasks, red teams will "challenge facts and explicit assumptions, look for implicit (unstated) assumptions, identifying cultural assumptions and developing targeted cultural questions for subject matter experts, challenging the problem frame (and proposing alternative frames), identifying cognitive biases and symptoms of underlying groupthink."[53] To this end, Micah Zenko identified three main varieties of red team techniques: simulations, vulnerability probes, and alternative analysis.[54] An organization may choose to employ one, two, or all three of these techniques depending on the circumstances.

---

[50] Mark Mateski, "Red Teaming: A Balanced View," *The Red Team Journal*, February 14, 2013, http://redteamjournal.com/2013/02/red-teaming-a-balanced-view/.

[51] University of Foreign Military and Cultural Studies, *The Applied Critical Thinking Handbook (formerly the Red Team Handbook)*, 1. The term "commander" is military terminology; however, it is synonymous with supervisor or team leader in the civilian world. This military definition closely matches the goals of security subcommittees in the security planning for major events.

[52] Ibid., 2.

[53] Ibid., 3.

[54] Zenko, *Red Team: How to Succeed by Thinking Like the Enemy*, XXI–XXII.

1. Red Team Techniques—Simulation Exercises

Simulations are often conducted in advance of significant events in an attempt to identify planning gaps and to anticipate how an adversary might behave. These simulations can vary in terms of complexity and realism depending on the circumstances of the event. Simulations may take the form of passive tabletop exercises or active operations complete with roleplaying actors. An example of major event simulations can be seen in the 2015 airspace exercise conducted by the North American Aerospace Defense Command (NORAD) in support of Super Bowl XLIX, a SEAR 1 event, held in Glendale, Arizona. Exercise Falcon Virgo was an airspace defense exercise designed to test the capabilities of the U.S. Air Force, Federal Aviation Authority (FAA), and the Customs and Border Patrol (CBP) to identify and intercept unauthorized aircraft from the temporary restricted airspace surrounding the stadium.[55] This exercise tested the security response to several simulated fixed-wing aircraft that violated the restricted airspace over Glendale in an attempt to improve response times and agency coordination to a real event.[56]

The DHS and partner homeland security agencies aggressively use this red team technique in the preparation for NSSEs and SEAR Level 1 events. The Federal Emergency Management Agency (FEMA), as the lead emergency response agency for NSSEs, is traditionally tasked with coordinating, designing, and executing these exercises. These exercises provide leadership an opportunity to test the command and control capability of the numerous assets involved in the security of a major event. An example of a tabletop exercise can be seen in New York City during the preparation for the September 2015 papal visit, which was designated a NSSE. This exercise brought more than 48 different local, state, and federal agencies together to test the operational plan and identify weaknesses in response to five unique scenarios including an active

[55] "NORAD Exercise Planned for Super Bowl XILX," January 26, 2015, http://www.norad.mil/News room/Press-Releases/Article/578766/norad-exercise-planned-for-super-bowl-xlix/.

[56] Ibid.

shooter, building collapse, major power outage, and a backpack improvised explosive device (IED).[57]

A more robust simulation example can be seen in the USSS' preparation for the 2017 presidential inauguration at its training facility in Beltsville, Maryland in January 2017. This red team simulation tested the agency on 40 different scenarios that could occur at various points along the historic parade route from the U.S. Capitol to the White House using dozens of agents, as well as roleplaying actors for the new president, first lady, and protestors.[58] Agents were tested on a range of possible situations including medical emergencies, armed assaults, and even risks posed from unmanned aerial vehicles (UAVs). This form of red team technique, whether in the form of tabletop exercises or full-scale simulations, is a significant part of the planning process for major events.

The red team technique of simulation exercises provides major event security planners with significant benefits. First, simulations enable security planners to test lines of communication between multiple agencies that often do not work together. These exercises enable local, state, and federal agencies to test their response capabilities to staged emergencies under elevated stress levels. This ability to add stress to both individuals and security plans enables leadership to anticipate weaknesses better in the security operation with no risk to the public or to their personnel. Of the three main varieties of red team techniques discussed in this thesis, simulation exercises are the most commonly accepted and used in the design and execution of NSSE and SEAR 1 events.

2. Red Team Techniques—Vulnerability Probes

Vulnerability probes are a class of red teaming in which role playing adversaries attack active defense systems to identify weaknesses in physical or cyber security.[59] This

---

[57] J. David Goodman, "Pope's Visit Poses a Security Test for New York," *The New York Times*, September 14, 2015, http://www.nytimes.com/2015/09/15/nyregion/pope-francis-visit-prompts-security-preparations-in-new-york.html?_r=0.

[58] Matthew Dean, "Secret Service Training in High Gear Ahead of Inauguration Day," *Fox News*, January 13, 2017, http://www.foxnews.com/politics/2017/01/13/secret-service-training-in-high-gear-ahead-inauguration-day.html.

[59] Zenko, *Red Team: How to Succeed by Thinking Like the Enemy*, XXII.

technique is employed across the federal government, as well as the private sector and can be conducted covertly or as part of a designed exercise. A prominent example was the 2015 DHS Office of Inspector General's probe of airport screening operations across the United States. Undercover agents successfully used disguises and false identities to smuggle fake weapons and explosives successfully past Transportation Security Administration screeners in 67 out 70 separate attempts.[60] Similarly, in the cyber-world, this technique is being employed extensively by the DOD. The 2016 program, titled "Hack the Pentagon," invited vetted civilians to attempt to discover vulnerabilities in the DOD's public non-mission critical systems during a controlled timeframe. The DOD offers successful participants cash bounties and awards for discoveries that lead to improvements in government systems.[61]

Unlike simulations, vulnerability probes have limited utility in the design and execution of security for major events for several reasons. First, NSSEs and SEAR Level 1 events traditionally last a short time and require a full deployment of available resources to secure the event.[62] Running a realistic vulnerability probe exercise during the actual event would draw limited resources away from a potential real-life incident response. Additionally, agencies and departments not familiar with each other's procedures will be working in close proximity increased the potential for a "friendly fire" or "blue on blue" situation.

Second, most major events involve significant numbers of attendees and non-attendee crowds. In most instances, it would be difficult to recreate this environment in a realistic manner. Lastly, major event security often affects the local community and economy in a negative manner. Road closures, disruption of mass transit, and lost revenue to local businesses in or near the security perimeter are all likely second-order

---

[60] Brian Bennett, "Red Team Agents Use Disguises, Ingenuity to Expose TSA Vulnerabilities," *Los Angeles Times*, June 2, 2015, http://www.latimes.com/nation/nationnow/.

[61] "Statement by Pentagon Press Secretary Peter Cook on DoD's "Hack the Pentagon" Cybersecurity Initiative," Release No: NR-070-16, March 2, 2016, http://www.defense.gov/News/News-Releases/News-Release-View/Article/684106/statement-by-pentagon-press-secretary-peter-cook-on-dods-hack-the-pentagon-cybe.

[62] One notable exception might be a major event that lasts for a long period of time or in a remote location, such as the 2002 Winter Olympics in Salt Lake City, Utah. In this circumstance, vulnerability probes may be a technique worth consideration.

consequences of major security events. An example of these effects can be seen in the 2004 Democratic National Convention in Boston, Massachusetts. The major event location, The Fleet Center, was located within 40 feet of Interstate 93 and directly over a commuter train station responsible for moving 24,000 passengers daily.[63] While these transportation routes were closed for the duration of the official event, closing them for a vulnerability test would present an additional hardship to the local community.

3. Red Team Technique—Analytical Analysis

Analytical analysis in the planning process requires the application of specific critical thinking techniques with the goal of improving overall decision making. The UFMCS curriculum contains dozens of different analytical techniques, but regardless of the type of technique used, red teams attempt to:

> Challenge facts and explicit assumptions, look for implicit (unstated) assumptions, identifying cultural assumptions and developing targeted cultural questions for subject matter experts, challenging the problem frame (and proposing alternative frames), identifying cognitive biases and symptoms of underlying groupthink.[64]

The Joint Forces Doctrine, responsible for instructing all branches of the armed forces, recognizes the value of these techniques and their benefits:

> Command red teams help commanders and staffs think critically and creatively; challenge assumptions; mitigate groupthink; reduce risks by serving as a check against complacency and surprise; and increase opportunities by helping the staff see situations, problems, and potential solutions from alternative perspectives.[65]

This variety of red teaming, unlike simulations and vulnerability probes, provides organizations with tremendous flexibility. Analytical techniques can be applied by an

---

[63] Esther Scott, *Security Planning for the 2004 Democratic National Convention (B)* (Cambridge, MA: Kennedy School of Government, 2005).

[64] University of Foreign Military and Cultural Studies, *The Applied Critical Thinking Handbook (formerly the Red Team Handbook)*, 3.

[65] United States Joint Force Development, *Command Red Team* (Joint Doctrine Note 1–16) (Washington, DC: United States Joint Force Development, 2016), http://dtic.mil/doctrine/notes/jdn1_16.pdf.

individual or group, from ad hoc or permanent teams, formally or informally, and during various phases of the planning process.[66]

An example of alternative analysis can be seen in the Central Intelligence Agency's (CIA) *Red Cell*. In the days after the 9/11 attacks, the CIA formed a group of contrarian thinkers called the Red Cell designed to "challenge the conventional thinking within the intelligence community and mitigate the threat of additional strategic surprises through the use of alternative analysis."[67]

An alternative analysis technique introduced at the beginning of this chapter is the devil's advocate. The use of an authentic devil's advocate has been noted as an effective countermeasure to the effects of groupthink.[68] Just like the papal version discussed in the beginning of this chapter, this technique requires a selected portion of the team to challenge weak assumptions and take a position opposite of the commonly held view. The U.S. military's Joint Doctrine Note states the goal of the devil's advocate as "to temporarily dismantle consensus, set aside preconceptions, and establish conditions that invite the staff to consider whether the problem is correctly framed."[69]

An example of the use of the devil's advocate technique in government planning can be seen in the Cuban Missile Crisis in 1962. President John F. Kennedy convened a small group of decision makers from the National Security Council to consider potential courses of action and then promptly removed himself from the decision-making process. Additionally, Attorney General Robert Kennedy was assigned to serve as the devil's advocate and specifically presented contrary ideas to force the group to consider and debate all potential options.[70]

---

[66] University of Foreign Military and Cultural Studies, *The Applied Critical Thinking Handbook (formerly the Red Team Handbook)*, 4.

[67] Zenko, *Red Team: How to Succeed by Thinking Like the Enemy*, 91.

[68] Sunstein and Hastie, *Wiser*, 115–118.

[69] United States Joint Force Development, *Command Red Team*, IV–2.

[70] Ben Dattner, "Preventing "Groupthink"," *Psychology Today*, April 20, 2011, https://www.psychologytoday.com/blog/credit-and-blame-work/201104/preventing-groupthink.

Premortem analysis is a red team technique first proposed by Gary Klein in his 1998 book, *Sources of Power: How People Make Decisions*, in which all group participants begin with the assumption that their proposed plan or operation has failed. Group members are then asked to identify and discuss potential reasons for that failure. This red team technique empowers participants to question the proposed operational plan and team assumptions. Premortem analysis:

> Legitimizes doubt according to Daniel Kahneman as well as encouraging all participants to search for threats to the proposed plan. According to The Applied Critical Thinking Handbook, this technique is effective because "the pull of groupthink, consensus, and a false sense of security is punctured, and is replaced by an active search aimed at preventing trouble later on.[71]

This technique "breaks the course of action through a divergent process that encourages objectivity and skepticism."[72]

C. CONCLUSION

The concepts and techniques of red teaming are being taught and increasingly used and accepted throughout the United States within the DOD, IC, and law enforcement community. While not all red team techniques are ideally suited for use in major event security design, the expanded use of analytical analysis has the potential to challenge organizational thought and assumptions. These techniques, however, need to be completed within the subcommittee framework used in the design and execution of security for major events.

---

[71] University of Foreign Military and Cultural Studies, *The Applied Critical Thinking Handbook (formerly the Red Team Handbook)*, 165.

[72] Ibid.

III. MAJOR SECURITY EVENTS—AN OVERVIEW

> Finally, the illusions of validity and skill are supported by a powerful professional culture. We know that people can maintain an unshakable faith in any proposition, however absurd, when they are sustained by a community of like-minded believers.[73]
>
> ~ Daniel Kahneman

Large national security events present U.S. homeland security professionals with planning, execution, and logistical challenges. The DHS takes a central role in classifying and designating events as either NSSE or SEAR level. This classification procedure can activate the full resources of the homeland security enterprise at all levels of government. This chapter addresses the historical origins and classification process of these events, as well as introducing the principal model for the planning and execution of major-event security planning.

The executive steering committee and subcommittee model is the prevailing organizational and decision-making structure used in the development of security for NSSE and SEAR Level 1 events. The planning process and framework for these events share many similarities; consequently, several of the same decision-making challenges exist for both types of events. The executive steering and subcommittee model marshals tremendous amounts of resources and ensures that roles and responsibilities between dozens of local, state, and federal agencies are clearly defined, all through small subcommittees of critical decision makers. It is within these subcommittees that structural and individual biases can affect the effectiveness of major security planning.

[73] Kahneman, *Thinking, Fast and Slow*, 217.

A. NATIONAL SPECIAL SECURITY EVENTS

Since the first NSSE in 1998, only 57 special events have received the official NSSE designation from the federal government.[74] Types of events that historically receive this designation include presidential inaugurations, major political conventions, world leader summits, such as the 2012 World Leader Summit in Chicago, and State of the Union addresses to the U.S. Congress. The NSSE designation triggers numerous federal agencies to facilitate planning, but it also allows the federal government to provide direct funding to local and state agencies for support.[75]

This designation is critical because the resources required to plan and execute these events far exceed the capabilities of individual federal agencies and would exhaust the resources of local and state agencies without specific funding. As an example, the U.S. Congress appropriated $50 million each for Cleveland, Ohio, and Philadelphia, Pennsylvania, to offset the security costs for the 2016 party conventions during the presidential election.[76] This $100 million investment was paid directly to the local and state agencies through grants managed by the Department of Justice and FEMA.[77]

The original framework responsible for the planning and execution of NSSEs was derived from the unclassified *Presidential Decision Directive 62: Protection against Unconventional Threats to the Homeland and Americans Overseas* (PDD 62) in 1998. Initially, the decision to recommend that an event receive the NSSE designation was made by an interagency counterterrorism working group with the U.S. Attorney General

---

[74] Total from 1998–2015 derived from United States Secret Service Memorandum dated February 12, 2015, obtained through a FOIA request posted on https://www.muckrock.com/foi/united-states-of-america-10/list-of-national-special-security-events-15602/. Total from 2015 to February 1, 2017 was derived from the USSS website: https://www.secretservice.gov/index.shtml.

[75] The USSS has no authorization to reimburse expenses for local and state agencies directly for their support.

[76] R. Sam Garratt and Shawn Reese, *Funding of Presidential Nominating Conventions: An Overview* (CRS Report No R46937) (Washington, DC: Congressional Research Service, 2016), 6, https://fas.org/sgp/crs/misc/R43976.pdf.

[77] Ibid., 5.

and Secretary of Treasury having final approval authority.[78] The USSS was designated as the lead federal planning and coordination agency, the FBI was designated as the primary counterterrorism and intelligence agency, and FEMA was tasked with disaster management at the federal level.[79] This directive provided the clear division of roles and responsibilities among the USSS, FBI, and FEMA that still exists today.[80] After the founding of the DHS, this directive was updated by the 2002 Homeland Security Presidential Directive 5 (HSPD-5), which codifies the Secretary of Homeland Security as the principal federal official for domestic incident management.[81] The original division of responsibilities among the USSS, FBI, and FEMA remained unchanged by HSPD-5.

The process by which an event receives the official designation of a NSSE begins when the governor of the host state contacts the Secretary of Homeland Security and requests that the event be evaluated. The host governor completes a written survey describing the event and the expected impact on the community. Once the DHS receives the request, the NSSE Steering Committee—composed of senior-level members of the USSS, FBI, FEMA, and other federal agencies—reviews the survey and makes a recommendation to the secretary.[82] While no specific rules exist for when an event receives the official designation, the DHS considers several factors, including the anticipated attendance of U.S. officials and foreign dignitaries, attendees, guests, and the crowd, and the potential historical or symbolic significance of an event.[83] Figure 1

---

[78] The White House, *Presidential Decision Directive NSC/62* (Washington, DC: The White House, 1998), http://fas.org/irp/offdocs/pdd/pdd-62.pdf. Declassified on March 18, 2014. Since the inception of the Department of Homeland Security, the final approving authority now resides with the Secretary of the Department of Homeland Security.

[79] These agencies typically lead the planning committees in their respective area of responsibility, but purposeful overlap does exist to ensure some degree of redundancy.

[80] *The Presidential Protection Act of 2000* codified the USSS' role as the lead planning agency for events designated as NSSEs in Title 18, United States Code 3056.

[81] Department of Homeland Security, *Homeland Security Protection Directive 5—Management of Domestic Incidents* (Washington, DC: Department of Homeland Security, 2003), https://www.dhs.gov/sites/default/files/publications/Homeland%20Security%20Presidential%20Directive%205.pdf.

[82] *Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment Field Hearing*, House of Representatives (2007) (written statement of Timothy J. Koerner, Assistant Director, United States Secret Service).

[83] Reese, *National Special Security Events*, 1.

outlines the decision-making process by which an event receives the official designation as a NSSE.

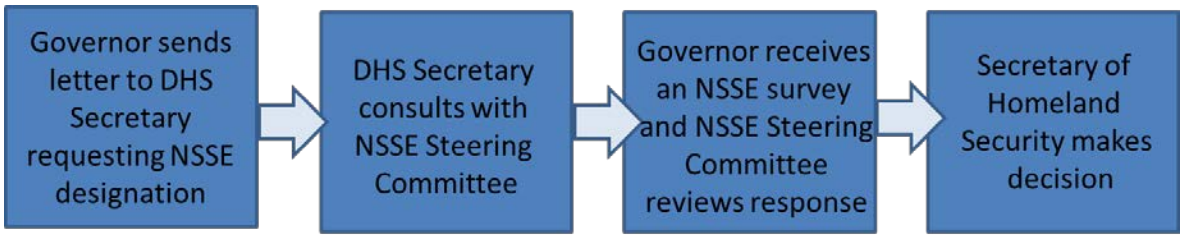

Figure 1. NSSE Designation Process.

Once the DHS Secretary has designated an event a NSSE, the executive steering committee begins formal security planning.[84]

B. SPECIAL EVENT ACTIVITY RATING LEVEL 1 EVENTS

In 2004, the DHS developed a risk-based methodology for identifying and categorizing events not designated as NSSEs. The DHS and its Office of National Protection and Programs Directorate (NPPD) developed the Special Event Working Group (SEWG) to assess events utilizing a methodological approach to risk. The SEWG consists of senior-level members from more than 50 federal agencies and is co-chaired by the NPPD, FBI, USSS, FEMA, and the DHS Office of Protection Coordination.[85] This group uses a combination of quantitative and qualitative data in an attempt to reduce subjectivity and improve consistency in ratings. Figure 2 shows the process by which the SEAR system reviews and classified events.

[84] Planning often begins before the official designation has been received for events that have a high likelihood for approval, such as presidential inauguration and presidential funerals.

[85] Department of Homeland Security, "Special Events Working Group" (lecture, online Fusion Talk, Department of Homeland Security, July 27, 2016).

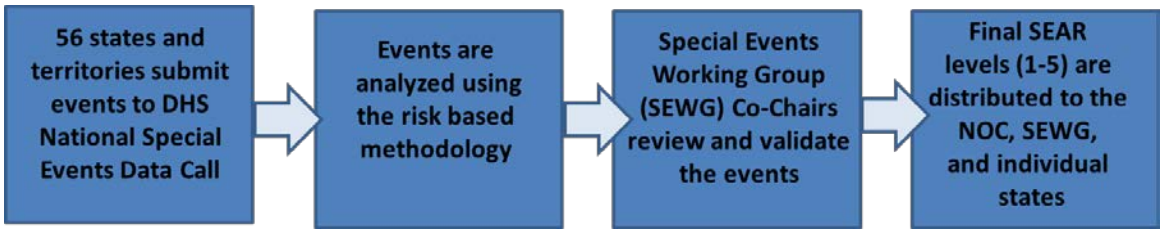

Figure 2. Special Events Rating Process.

Each year, states are invited to submit their events to the DHS in the National Special Events Data Call.[86] The NPPD and their SEWG assess each event utilizing a risk-based methodology and issue a SEAR from 1 to 5 in descending order of perceived risk. Figure 3 shows examples of events and their SEAR level.

Level 1	• Significant national and/or international importance • May require extensive federal interagency support	• Super Bowl • United Nations General Assembly • Rose Parade/Rose Bowl
Level 2	• Significant events with national and/or international importance • May require some national level federal support	• Papal Visit to the US/MX Border-El Paso • Boston Marathon • DC Fourth of July
Level 3	• Events of national and/or international importance • Requires only limited federal support	• Chevron Houston Marathon • Texas Motor Speedway NASCAR Races
Level 4	• Limited national importance • Handled at the state/local level	• Cotton Bowl • South by Southwest/SXSW
Level 5	• Events may be nationally recognized but generally have only state/local importance • Normally handled at the local level	• Sun City Music Festival • MLB: 2016 Houston Astros • Star of Texas Fair & Rodeo

Figure 3. Examples of SEAR Events at Each Level.[87]

SEAR events rated a 1 and 2 are assigned a principal federal coordinator and potentially an assistant federal coordinator responsible for coordinating the federal assets

[86] Ibid.

[87] Source: Department of Homeland Security, "Special Events Working Group."

and support for these events and representing the Secretary of Homeland Security.[88] SEAR events rated 4 or 5 receive virtually no federal support, as they have been deemed outside the level of national significance.[89] No matter the SEAR rating, and the eventual level of federal support, the overall coordination and responsibility for the design and security resides with the local and state agencies. Once the SEWG has issued a SEAR level, all planning and coordination is transferred to the local area and to the executive steering committee responsible for each event.

C. EXECUTIVE STEERING COMMITTEE AND SUBCOMMITTEE PLANNING PROCESS

Once an event has received the NSSE designation or been rated as a SEAR Level 1, the executive steering committee and subcommittee planning process begins. Unlike NSSEs, membership in SEAR Level 1 event committees and subcommittees traditionally is composed primarily of local and state government agencies. The planning cycle timeline varies by location and complexity of the event but is usually longer than 12 months.[90] As an example, the security planning for the 2012 Democratic National Convention in Charlotte, North Carolina, began 19 months in advance of the event's start date.[91]

NSSE executive steering committees traditionally consist of the principal federal coordinator, USSS, FBI, FEMA, private partner entities, host city and state senior-law

---

[88] *Homeland Security Presidential Directive–5* designates the Secretary of Homeland Security as the principal federal coordinator for all domestic incident management. The Secretary then delegates this responsibility.

[89] Please refer to James Gehring, "Sports Venue Security: Public Policy Options for SEAR 4–5 Events" (master's thesis, Naval Postgraduate School, 2014) for an excellent overview on the risks to SEAR 4 and 5; the premise being that NSSEs and Level 1 events are hardened targets and terrorists will be forced to target the less well-protected Level 4 and 5 events.

[90] Planning timelines vary by the type of event and can range from years (2002 Olympic Games in Salt Lake City, Utah) to days (U.S. Presidential funerals, such as the 2006 funeral of Former President Gerald Ford).

[91] Vivian Chu and Tammy Felix, *Command, Control, and Coordination: A Quick-Look Analysis of the Charlotte-Mecklenberg Police Department's Operations During the 2012 Democratic National Convention* (IQR-2013-U-004229) (Washington, DC: Department of Justice, Bureau of Justice Assistance and Alexandria, VA: CNA Analysis & Solutions, 2013), 45, https://www.bja.gov/Publications/2012-DNC-Quick-Look.pdf.

enforcement, fire, and emergency management officials.[92] The purpose of these steering committees is to identify priority risks and organize subcommittees to address specific areas of concern. Each unique subcommittee reports to the executive steering committee ultimately responsible for approving its operational plan.

For example, the 2012 Republican National Convention held in Tampa, Florida, and the 2012 Democratic National Convention in Charlotte, North Carolina, each had 24 individual planning subcommittees reporting back to the overall executive steering committees.[93] This approach to managing assets and organizations ensures that roles and responsibilities are clearly defined and minimizes the chance for duplication of efforts.

The following list outlines the subcommittees that participated in the 2012 Republican National Convention in Tampa:

1. Airport
2. Airspace Security
3. Civil Disturbance
4. Consequence Management
5. Counter Surveillance
6. Credentialing
7. Crisis Management
8. Critical Infrastructure Protection
9. Crowd Management
10. Dignitary/VIP Protection
11. Explosive Device Response
12. Fire/Life Safety/Hazardous Materials
13. Health/Medical
14. Intelligence/Counterterrorism
15. Interagency Communications
16. Legal/Civil Liberties
17. Logistics/ Asset Identification
18. Public Affairs
19. Staffing and Housing
20. Tactical
21. Technology
22. Training
23. Transportation/Traffic
24. Venue Security[94]

Each NSSE subcommittee has a chair and several co-chairs consisting of a member of the USSS, another federal agency with specific subject-matter expertise, and a

[92] The committees for NSSE and SEAR Level 1 events have a slightly different composition; however, the framework is the same. As an example, the USSS usually plays no direct planning role in SEAR Level 1 events.

[93] Denise Rodriguez-King and Tammy Felix, *Command, Control, and Coordination: A Quick-Look Analysis of the Tampa Police Department's Operations During the 2012 Republican National Convention* (IQR-2013-U-004228) (Washington, DC: Department of Justice, Bureau of Justice Assistance and Alexandria, VA: CNA Analysis & Solutions, 2013), 42, https://www.bja.gov/Publications/2012-RNC-Quick-Look.pdf.

[94] Ibid.

local or state law enforcement representative with critical knowledge of the local community.

The subcommittees for SEAR Level 1 events are similar in scope, but are staffed primarily by local and state homeland security officials. It is specifically within these subcommittees that the majority of operational, tactical, and strategic planning occurs for major events.

D. SUBCOMMITTEE MODEL—INSTITUTIONAL AND INDIVIDUAL DECISION-MAKING TRAPS

The subcommittee process employed in the planning of security for major events is vulnerable to decision-making errors, biases, and institutional blindness. This section analyzes the organizational framework of major event security subcommittees and identifies both institutional and individual decision-making errors.

1. Institutional—Groupthink

The security subcommittees operate in a framework specifically designed to separate decision makers according to areas of specialization. While this organizational structure is effective in breaking up the otherwise overwhelming amount of work and defining areas of responsibility, it also limits, or insulates, each subcommittee from each other. This information "silo effect" minimizes the exposure of subject-matter experts and can lead to planning gaps between subcommittees.

NSSEs and SEAR Level 1 events are held in a set of geographic locations throughout the country on a random rotating basis.[95] In most instances, specifically in NSSEs, representatives from the USSS, FBI, or FEMA chair or co-chair these committees. These representatives are selected from a very small group of individuals and often complete more than one event in a career. The great majority of planners on the subcommittees are participating in their first major security event with the exception of these USSS, FBI, and FEMA representatives. These planners, by virtue of their real or

[95] Notable exceptions include the District of Columbia (State of the Union address and Presidential Inaugurations) and New York City, New York (United Nations General Assembly annual meetings).

perceived historical experience, may inadvertently stifle open debate and critical thinking by all members of the subcommittee.

Committee members may defer to the "expert" planner's thoughts and opinions out of social pressure, or conversely, the opinions and ideas of less experienced planners may not receive proper consideration. Ephraim Kam explored the relation between "expert" and "non-expert" decision makers in the intelligence community in his 1988 book, *Surprise Attack: A Victim's Perspective*. In Kam's analysis of 11 major surprise attacks, he posited, "Experts within an organization tend to reject non-experts' warnings and opinions, the experts' argument is that they are in the best position to evaluate information and developments."[96] A chair and co-chair participant's firmly held opinions could have an oversized influence that could steer the group to a poor decision.

While the organizational framework for major events is well established, no formal process is in place for the development of security plans for NSSEs and SEAR Level 1 events within the individual subcommittees. Each subcommittee is responsible for designing a formal plan and providing it to the executive steering committee with a formal plan; however, the system by which decisions are made depends entirely on the committee chairs. Janis refers to this absence of planning process as a "lack of norms requiring methodical procedures in decision-making."[97] If Janis is correct, this lack of a methodical decision-making process could lead to groupthink within the security subcommittee. With no formal process to evaluate and consider various points of view, a subcommittee chair may simply ignore or discount contrarian thoughts and ideas.

The final and most critical structural antecedent of groupthink is the overall homogeneity of the subcommittee members. Essentially, the more *esprit de corps* a group possesses, the greater the danger of groupthink.[98] *Esprit de corps* is typically considered a positive trait for law enforcement agencies because it promotes discipline and

---

[96] Ephraim Kam, *Surprise Attack: A Victim's Perspective* (Cambridge, MA: Harvard University Press, 1988), 161.

[97] Janis, *Groupthink: Psychological Studies of Policy Decision and Fiascos*, 244.

[98] Ibid., 245.

camaraderie; yet, it creates a sense of "us versus them."[99] This division could be composed of the actual entire subcommittee, a small group within the subcommittee, or even the agency itself. Additionally, members of a particular agency may not want to risk offending a partner-agency's representative and allow an otherwise objectionable decision to proceed uncontested.

Major security event subcommittees traditionally consist of members of local, state, and federal law enforcement, fire and life safety, and military organizations. An example would be fire and life safety personnel perceiving law enforcement officials as outsiders, and therefore, deserving of lower status within the group. Additionally, members of local and state law enforcement departments may resist ideas presented by "outside" federal authorities. This perceived lower status of the sub-group within the committee could lead to an imbalance in the decision-making process and greater importance placed on the thoughts of the "in-group" members.

2. Individual—Heuristics and Planning Fallacies

Ideally, homeland security professionals wish to control and know as many planning variables as possible when designing the security for a major event. Many critical factors are simply unknown or are only partially known during the design of security plans. Planners can anticipate the total number of attendees to an affair based on the size of the venue and historical documentation, but it is only one piece of the puzzle. Additional factors include the time of the crowd's arrival, as well as the direction of travel when approaching and departing the event. In this grey area of planning, individuals often resort to mental shortcuts, or heuristics, to "fill in the blanks." These heuristics can be helpful, but can lead to faulty and systemic planning assumptions and errors.[100]

---

[99] Ricciutti, "Groupthink: A Significant Threat to the Homeland Security of the United States."

[100] Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science* 185, no. 4157 (September 27, 1974): 1124.

E. AVAILABILITY HEURISTIC

The availability heuristic is a mental shortcut used by individuals when considering questions about probability.[101] Decision makers assume an event is more likely to occur if a similar event has recently happened or is easy to recall regardless of contradictory information. One example would be making decisions based on the desire to avoid "another 9/11." This process leads to planning for events that have a very low likelihood of occurring based solely on the ease of which a similar event can be recalled.

This heuristic is also closely related to the concept of anchoring and adjusting. Anchoring is the process by which individuals make estimates on starting values and adjust from this initial value as more complete information becomes available.[102] Initial estimates, or starting points, can be formed after reviewing the circumstances surrounding an event or historical knowledge, but Tversky and Kahneman suggest that future adjustments are often insufficient and demonstrate a bias toward the initial starting point regardless of new information.[103]

F. REPRESENTATIVENESS HEURISTIC

A second individual heuristic that can negatively impact decision makers in major security events is the representativeness heuristic. Tversky and Kahneman define this heuristic as follows, "When A is highly representative of B, the probability that A originates from B is judged to be high."[104] This mental shortcut leads decision makers to wrongly predict the chances of a low probability event by drawing comparisons to other similar events.[105] This heuristic can lead to security planners overstating potential risk and focusing limited resources on highly unlikely events. Inversely, this heuristic can lead planners to make false assumptions about their events when comparing them to similar events from recent past. This concept is important to consider for events that

---

[101] Sunstein and Hastie, *Wiser*, 44–45.

[102] Tversky and Kahneman, "Judgment under Uncertainty: Heuristics and Biases," 1128.

[103] Ibid.

[104] Ibid., 1124.

[105] Kahneman, *Thinking Fast and Slow*, 151.

periodically occur in the same geographic location, such as the United Nations General Assembly in New York City, the annual State of the Union Address to Congress, and the presidential inauguration held every four years in Washington, DC. Additionally, agencies and departments may assign the same personnel for these events from one year to another paradoxically increasing the chances of both the representativeness and availability heuristics creeping into the planning for events.

IV. MAJOR SECURITY PLANNING—2009 PRESIDENTIAL INAUGURATION

> They had months to prepare. … And their planning was woefully inadequate and put thousands of people at risk.[106]
>
> ~ Anonymous Purple Tunnel Victim

This chapter introduces a case study into the crowd-management issues that plagued the 2009 presidential inauguration. This case study also provides a glimpse into the complexity and multi-faceted process in which major event security is designed and executed.

On November 4, 2008, Senator Barack Obama was elected as the 44th President of the United States. Although his inauguration would not occur until January 2009, the USSS had begun initial planning and coordination as far back as May 2008 for the event.[107] Media outlets estimated that approximately two million people would converge on Washington, DC, the U.S. Capitol grounds, and the National Mall to witness the historic Obama inauguration.[108] These attendance estimates far surpassed the 2005 presidential inauguration crowd of 400,000, and if true, would be the largest crowd to ever attend an inauguration or any other event in the District of Columbia.[109]

---

[106] Laura Rozen, "Purple Tunnel of Doom After-action Report: "Survivors" Offer Lessons Learned," *Foreign Policy*, January 21, 2009, http://foreignpolicy.com/2009/01/21/purple-tunnel-of-doom-after-action-report-survivors-offer-lessons-learned/.

[107] United States Secret Service, *Multi-Agency Response to Concerns Raised by the Joint Congressional Committee on the Inaugural Ceremonies for the 56th Presidential Inauguration* (Washington, DC: United States Secret Service, 2009), 7. This report was initially marked For Official Use Only (FOUO); however, a redacted version was released to the public subsequent to a Freedom of Information Act (FOIA) request on March 19, 2010.

[108] Lauren Kornreich, "Arrive Early, Wear Comfy Shoes on Inauguration Day," *CNN*, January 19, 2009, http://www.cnn.com/2009/TRAVEL/01/18/inauguration.travel/index.html. Event planners made the decision to open the entire National Mall to attendees. Individuals did not need a ticket and were not security screened in this area.

[109] "Official Inauguration Crowd Estimate: 1.8 Million," January 22, 2009, http://politicalticker.blogs.cnn.com/2009/01/22/official-inauguration-crowd-estimate-18-million/.

U.S. intelligence agency assessments posited that the inauguration would be an appealing target for domestic and international terrorists due in part to the swearing in of the nation's first African-American president.[110] The protection of the attendees and the ceremony marking the nation's peaceful transition of power needed the full resources of local, state, and federal homeland security agencies. Despite months of planning and years of experience in securing similar events, several thousand ticket holders who arrived in Washington never made it into the inauguration ceremony.[111] These ticketed guests were not able to arrive at the checkpoints for entry into the event because of a confluence of factors that should have been anticipated during the planning process.

A. AMERICA'S PEACEFUL TRANSITION OF POWER

The swearing-in ceremony was scheduled to begin at 11:30 a.m. on January 20, 2009, on the West Front of the U.S. Capitol complex. Months of security coordination, walk-throughs, and planning between dozens of different local, state, federal, and DOD agencies, as well as staff and private entities, were now complete. A full-scale practice inauguration, complete with actors playing the president and first lady, was held in advance to ensure that all staff and military entities knew their exact role and to practice the coordination and timing required for the historic event.[112] The Executive Steering Committee (ESC) conducted and completed several tabletop exercises that tested the strength of the security plan in the weeks leading up to the event.[113] On January 11, 2009, the Joint Congressional Committee on Inaugural Ceremonies (JCCIC) published a news release with detailed instructions for attendees including a map of the downtown area with recommended mass transportation options, entry locations, and security-related

---

[110] The Associated Press, "Feds Say Inauguration an Attractive Terrorist Target," *NBC News*, January 7, 2009, http://www.nbcnews.com/id/28547871/ns/politics-inauguration/t/feds-say-inauguration-attractive-terrorist-target/#.V_k1wsZFDIU.

[111] Robin Abcarian, "They Came for the Inauguration but Got Stuck in a Tunnel," *The Los Angeles Times*, January 23, 2009, http://articles.latimes.com/2009/jan/23/nation/na-angry-inauguration-goers23.

[112] Michael E. Ruane and Nikita Stewart, "Practice Inauguration Lacks Some Pomp and the VIPs," *The Washington Post*, January 12, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/01/11/AR2009011100625.html?sid=ST2009011102548. This practice focused on the ceremonial events of the inauguration and did not include an activation of the security component.

[113] United States Secret Service, *Multi-Agency Response to Concerns Raised by the Joint Congressional Committee on the Inaugural Ceremonies for the 56th Presidential Inauguration*, 8.

information designed to assist those attending the event.[114] The Washington Metropolitan Area Transit Authority (WMATA) coordinated bus and Metro rail service to begin at 4:00 a.m. to accommodate the unprecedented crowds coming into Washington, DC.[115]

The U.S. Capitol Subcommittee, one of the 23 unique security subcommittees working in unison to protect the NSSE, was responsible for the security planning for all events held on the grounds of the Capitol including the swearing in ceremony. The subcommittee was chaired by the U.S. Capitol Police (USCP) and co-chaired by the USSS. The challenge for this group was the immense crowd that would descend upon the Capitol and ensuring that those ticketed guests could be security screened within the allotted time.

The USSS was responsible for the planning, preparing, and conducting all screening operations on the Capitol grounds.[116] The agency, relying on historical experience both from previous inaugurations and other major events, planned to use walk-through magnetometers. The USSS established a screening rate of 700 guests per hour for the purple section having the knowledge of the exact number of ticketed guests.[117] The U.S. Capitol Security Subcommittee designed and implemented a new "metering" system to ensure the crowd would flow into the security screening areas in a controlled manner. This system was designed to ensure that the screening area would not be overrun by a large crowd and to minimize the potential for injury to members of the crowd.

B. THE PURPLE TUNNEL OF DOOM

Only 241,738 lucky attendees received a dedicated color-coded ticket to the historic ceremony at the Capitol.[118] Ticket colors coincided with designated seating and

---

[114] See Figure 1.

[115] "Metro Outlines Inauguration Day Service Plans," accessed December 22, 2016, https://www.wmata.com/about/news/pressreleasedetail.cfm?ReleaseID=2350.

[116] United States Secret Service, *Multi-Agency Response to Concerns Raised by the Joint Congressional Committee on the Inaugural Ceremonies for the 56th Presidential Inauguration*, 12.

[117] Ibid., 15.

[118] Ibid., 11. The rest of the crowd would not need a ticket to observe the swearing-in ceremony or parade and space was not reserved.

standing areas around the Capitol: yellow (19,269), orange (17,469), blue (52,500), purple (52,500), and silver (100,000).[119] A map of the Capitol grounds and color-coded gates are shown in Figure 4.

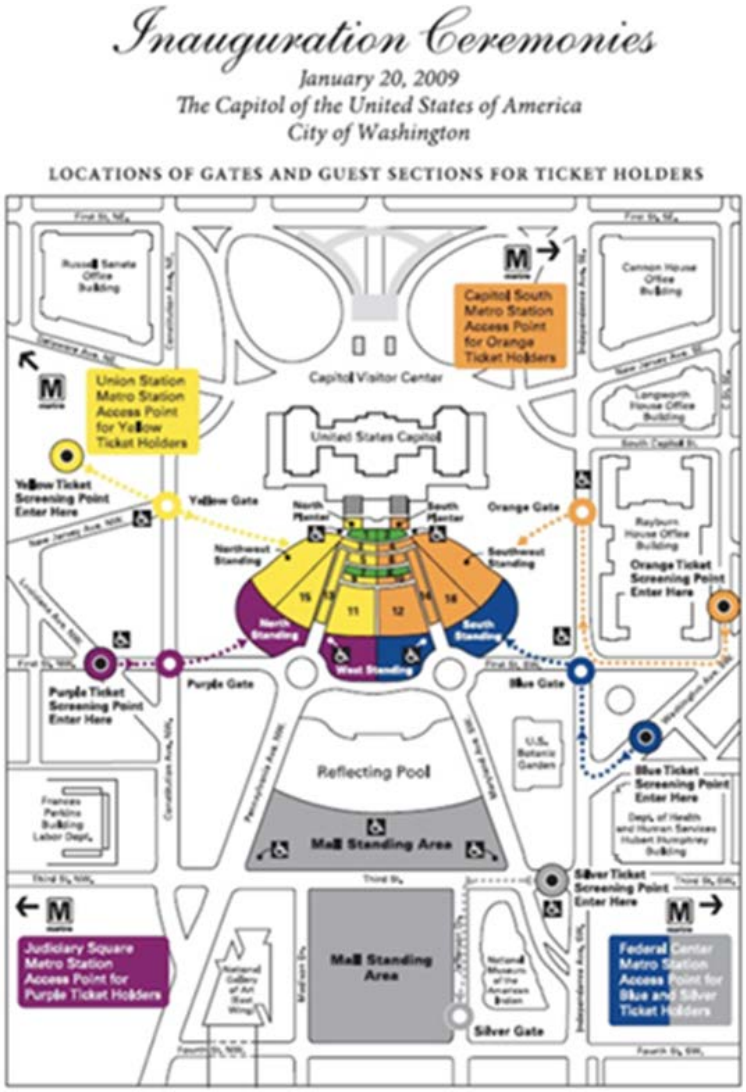

Figure 4. JCCIC Map of the U.S. Capitol on Inauguration Day.[120]

[119] United States Secret Service, *Multi-Agency Response to Concerns Raised by the Joint Congressional Committee on the Inaugural Ceremonies for the 56th Presidential Inauguration*, 11.

[120] Source: Joint Congressional Committee on Inaugural Ceremonies, *JCCIC Releases Map and Ticket Information for Inaugural Swearing-In Ceremonies* (Washington, DC: Joint Congressional Committee on Inaugural Ceremonies, 2009), http://www.wmata.com/getting_around/metro_events/ticket-map_release.pdf.

A dedicated color-coded entry and security screening location was prepared to open and begin entry of the ticketed public at the published time of 8:00 a.m. or as soon as the security searches of the U.S. Capitol were complete or whichever occurred first.[121] In reality, the purple gate was officially open for screening at 7:33 a.m. and did not close until almost 12:00 p.m.[122]

Security planners were aware of the exact number of ticketed guests who would need to be screened and the allotted time to complete this task to ensure all ticketed attendees were inside the viewing zone. Despite these known factors, crowd entry complaints began before President Obama took the official Oath of Office, as calls and emails poured into various command posts across the city.[123] Social media websites erupted with posts from ticket holders who never made it into the event despite waiting in line for hours in the near-freezing temperatures.[124]

According to media reports the day after the inauguration, several thousand purple-ticket holders were stuck in line for hours in the 3rd Street, N.W., underground tunnel located between Constitution Avenue and Independence Avenue and did not gain entry into the Capitol events.[125] Within one day, a Facebook page entitled "Survivors of the Purple Tunnel of Doom" formed and had more than 1,000 members.[126] This page grew in membership to over 5,000 members in less than one week.[127] Comments on this

---

[121] United States Secret Service, *Multi-Agency Response to Concerns Raised by the Joint Congressional Committee on the Inaugural Ceremonies for the 56th Presidential Inauguration*, 16.

[122] Abcarian, "They Came for the Inauguration but Got Stuck in a Tunnel."

[123] Mary Beth Sheridan and Pamela Constable, "Inaugural Missteps and Miscalculations," *Washington Post*, January 25, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/01/24/AR2009012401928.html. According to the "Multi-Agency Response," purple and blue tickets holders were granted entry through any security gate at 10:45 a.m. regardless of color-coding in an attempt to alleviate the crowd density.

[124] Jason Linkins, "Purple Ticket Turmoil Explained: What Happened on Inauguration Day," *The Huffington Post*, updated May 25, 2011, http://www.huffingtonpost.com/2009/01/23/purple-ticket-turmoil-wha_n_160150.html.

[125] Pamela Constable and Mary Beth Sheridan, "And Then we Knew It Was Too Late," *Washington Post*, January 21, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/01/20/AR2009012003362.html.

[126] Rozen, "Purple Tunnel of Doom After-action Report." This Facebook page has over 5,000 members.

[127] Kristin Nicole, "Purple Tunnel of Doom Gets Authority's Attention," *Social Times*, January 27, 2009, http://www.adweek.com/socialtimes/purple-tunnel-doom-facebook-group/306741.

Facebook page described the problem and provided dozens of first-person accounts of the crowd management issues.

> Arrived at 6:30 am. DIRECTED INTO THE TUNNEL BY TWO POLICE OFFICERS WHO CHECKED OUR TICKETS. Waited, waited, waited with the 1000s of others. No police, no volunteers, no porta-potties, no water, no food. Inched forward with increasingly agitated, though civilized, mob.[128]

> I was among the thousands of purple ticket holders who had their Inaugural dreams dashed away by poor planning, lack of official personnel and an overall logistical failure by the police departments (many from out of town and had absolutely no information), the Inaugural Committee and Secret Service.[129]

> We had purple tickets and arrived at the line around 7:50 AM. Seven of my friends and I were crushed in a dangerous mob in a 15 degree chill for five hours at D and first Sts. NW. We probably moved ten feet within the course of two hours at one point. There was absolutely zero crowd control. We witnessed old people, people in wheelchairs, and children all being crushed.[130]

Public outrage grew as the story of the thousands of stranded guests received an increasing amount of media attention in the aftermath of the inauguration. On January 21, 2009, Senator Dianne Feinstein, Chair of the JCCIC, officially requested that the USSS as the NSSE planning lead convene a multi-agency investigation into the events surrounding the crowd management at the U.S. Capitol. Senator Feinstein requested this investigation specifically to review the 3rd Street tunnel "where thousands of people were stuck for several hours and apparently without any law enforcement presence."[131] Not only did these ticketed guests not gain entry into the event, but they were placed into a situation that could have devolved into a dangerous public safety issue. Despite the

---

[128] Sara Willbrich, Facebook post, "Survivors of the Purple Tunnel of Doom," January 22, 2009, https://www.facebook.com/groups/61444130820/.

[129] Shelley Max, Facebook post, "Survivors of the Purple Tunnel of Doom," January 22, 2009, https://www.facebook.com/groups/61444130820/.

[130] Megan Lantz, Facebook post, "Survivors of the Purple Tunnel of Doom," January 21, 2009, https://www.facebook.com/groups/61444130820/.

[131] David Nakamura, "Sen. Feinstein Launches Investigation into Ticket Fiasco," *Washington Post*, January 21, 2009, http://voices.washingtonpost.com/inauguration-watch/2009/01/sen_feinstein_launches_investi.html.

activation of the full force of the homeland security enterprise, this event was marred by the failure to consider the behavior of an integral piece of the security puzzle: the crowd.

C. ASSUMPTION—THE ENEMY OF SECURITY PLANNING

The USSS, in conjunction with the USCP, United States Park Police, and the Metropolitan Police Department, completed the requested Congressional report in March 2009 and outlined several planning and execution errors that led to the crowd-management issues during the inauguration.[132] This report examined several factors of the crowd management issue to include the number of magnetometers, amount of time per individual search, and the size of the physical openings at each gate to determine why these guests did not gain entry into the event.[133]

This report advised that no checkpoints were closed at the U.S. Capitol due to lack of space available *inside* the event.[134] This situation indicates that the system of screening and admitting ticketed guests had broken down. The failure to anticipate the number of non-ticketed guests who migrated into the security screening area was "drastically underestimated by planners."[135] Removing these non-ticketed guests from the queue required additional time in the sorting and screening process and kept large numbers of ticketed crowds from reaching the screening locations. Additionally, this significant increase in the crowd surrounding the entry points forced people to migrate into the 3rd Street tunnel where no law enforcement, medical, or restroom services were staged to support them.

The subcommittee focused its planning and attention on screening ticketed guests to gain entrance into the event and expressed concerns to the ESC and the JCCIC about the space available *inside* the secure area on the Capitol.[136] This subcommittee, however,

---

[132] This report made recommendations for improvement in many areas of the event planning and execution and not simply crowd management.

[133] United States Secret Service, *Multi-Agency Response to Concerns Raised by the Joint Congressional Committee on the Inaugural Ceremonies for the 56th Presidential Inauguration*, 15–26.

[134] Ibid., 22.

[135] Ibid.

[136] Ibid., 10–11.

never anticipated the behavior of the larger non-ticketed crowd on the *outside* of this secured event. Planners on this subcommittee had never seen a crowd as big as the one that descended on the District that day and simply had no historical frame of reference for its potential behavior. Previous inaugurations' security plans provided little assistance, and in fact, may have proved to be an impediment to the crowd management planning by cementing assumptions on the behavior of the non-ticketed crowd.

The crowd management failure that affected the 2009 presidential inauguration exemplified several of the observable consequences studied by Janis. By not factoring the behavior of the crowd, both ticketed and non-ticketed, the planners failed to examine the potential risks to their plan. Additionally, they demonstrated an incomplete survey of alternates by using the exact same screening locations from previous inaugurations even when the crowd size was expected to be significantly larger than the 2005 presidential inauguration. This failure to examine options, consequences, and risk is a hallmark of poor decision making and groupthink.

V. RED TEAM PITFALLS AND TRAPS

> I will look at any additional evidence to confirm the opinion to which I have already come.[137]
>
> ~ Lord Hugh Molson

This chapter identifies methods and techniques that could have been employed to assist in identifying the crowd management issues that marred the 2009 presidential inauguration. The techniques of red team analysis can challenge planning assumptions, reveal overlooked vulnerabilities and opportunities, identify second- and third-order effects, and provide alternative courses of action to planners.[138] These potential benefits, however, are only derived and maximized when the process of red teaming is completed in a structured and formal process conducted by trained and educated professionals.[139] Several "best practices" and pitfalls have been identified in the execution of red teaming as well. This chapter introduces those implementation difficulties that exist and outline ways in which red team techniques can be marginalized.

A. THE PURPLE TUNNEL OF DOOM—ANALYTICAL RED TEAM TECHNIQUES

With the benefit of hindsight, the 2009 presidential inauguration crowd management errors seem clear. Ample warning was given that the overall crowd size would be at historic levels and that the number of ticketed guests who would actually attend the swearing in ceremony would be higher than a typical inauguration.[140] Planners relied on their historical knowledge base and made adjustments to security procedures to accommodate the increased crowd.[141] Relying on previous inauguration plans and

---

[137] Tavris and Aronson, *Mistakes Were Made*, 21.

[138] Gregory Fontenot, "Seeing Red: Creating a Red-Team Capability for the Blue Force," *Military Review*, September–October 2005, 5.

[139] Ibid., 4.

[140] United States Secret Service, *Multi-Agency Response to Concerns Raised by the Joint Congressional Committee on the Inaugural Ceremonies for the 56th Presidential Inauguration*, 20–23.

[141] Ibid., 14–30.

experiences gained through other major events proved little value and may have actually hindered the group's ability to consider unique risks and recognize planning assumptions. Would the application of analytical red team techniques to the inauguration planning process have improved the results of the 2009 presidential inauguration?

Two analytical red team techniques that could have potentially been used in the subcommittee process for this event are the devil's advocate and the premortem analysis, both of which were introduced in Chapter II. The devil's advocate role, whether officially designated or developed organically, would serve to counter assumptions made by the group. In this particular event, the assumption on the number of non-ticketed guests who would attempt to gain entry into the ceremony was significantly underestimated.[142] The devil's advocate would ideally challenge that assumption and attempt to convince the overall group of the potential for a larger crowd that would be too dense to allow for ticketed guests to enter the screening area.

A premortem analysis would involve the entire planning subcommittee and would push each member to consider ways in which the event would fail. The expected historic crowd size was a significant concern and allowing the group the freedom to consider failure might have led to this issue being identified prior to the event itself instead of when it was too late to make a meaningful adjustment.

Like all red team techniques, these two proposed analytical options require members to be open to feedback and adjustment for the suggestions to be of value. Even with the adoption of one or both of these analytical techniques, it remains unclear if the suggestions and concerns identified would have been accepted and implemented by agency leadership. Conceptually, the potential for red team analysis to be impactful to major-event security planning is present, but these techniques can be difficult to execute.

B. RED TEAM EXECUTION TRAP

While no formal quantitative study has been completed on the efficacy of red team techniques within DOD operations, several "best practices" and pitfalls have been

[142] United States Secret Service, *Multi-Agency Response to Concerns Raised by the Joint Congressional Committee on the Inaugural Ceremonies for the 56th Presidential Inauguration,* 22.

identified.[143] These execution traps need to be considered prior to the formal adoption of these techniques into the security planning for major events, as each has the potential to reduce the overall effectiveness of red teaming.

1. Acceptance by Senior Leadership

The senior leaders of an agency or department must be open to challenge and criticism. For many agencies, this process is difficult as decision-making biases are inherently difficult to self-identify for organizational and individual reasons. Organizations experienced in "grading their own homework" may resist having their planning decisions exposed to outside review and criticism.[144] Leadership must understand that the operation suffers from vulnerabilities that can potentially be minimized through the use of red team techniques.[145] Senior management must also provide the necessary resources and access to planners for red teaming to be valuable. In many instances, organizations only embrace analytical red teaming after a significant error or event has occurred. In the days after the terrorist attacks of 9/11, the CIA formed a group of contrarian thinkers called the Red Cell, which was designed to provide alternative analysis.[146]

An example of red teaming not accepted by senior management can be seen in the FAA and highlighted in Zenko's *Red Team*. The FAA instituted a small red team to conduct threat and vulnerability assessments only after the Pan Am 103 bombing over Lockerbie, Scotland that killed 270 passengers in 1988.[147] This small red team, often consisting of only four or five total agents, was tasked with conducting vulnerability probes and assessments at domestic and international airports.[148] This team was formed with "no foundational mission statement or guidance document" to "govern the conduct

---

[143] Zenko, *Red Team: How to Succeed by Thinking Like the Enemy*, 231–232.

[144] Ibid., 3.

[145] Ibid.

[146] Ibid., 91.

[147] Ibid., 3.

[148] Ibid., 118. This team was originally scheduled to be 18 agents, but never grew beyond eight due to lack of funding.

of the red team's operations, the scope of its activities, or the management of its findings."[149]

Red team members consistently identified vulnerabilities in airports and forwarded their results to the senior leadership of the FAA and to the associate administrator of the Office of the Civil Aviation Security (CAS). These organizations had the authority to levy fines and order remedial action as a result of the red team findings. Despite identifying significant vulnerabilities in airports around the world and reporting them to their senior leadership, little or no significant upgrades were made from 1991 until 2001. Red team members, frustrated by years of inaction, took their results to the *U.S. News & World Report* and provided detailed information for a magazine article that appeared in February 2001.[150]

The FAA red team was disbanded just days after the events of 9/11 with at least one team member filing a whistleblower disclosure with the Office of Special Counsel against his agency.[151] The FAA red team identified significant security vulnerabilities in aviation security; however, senior leadership was either unwilling or unable to make significant improvements prior to the events of 9/11. An organization must recognize the critical nature of red teaming to benefit fully from this technique prior to spending significant amounts of time, energy, and resources on poorly conceived plans.

2. Proper Team Composition and Staffing

Second, organizations should properly recruit, select, and train individuals to participate in red teaming activities. The ability to think creatively and communicate potentially negative findings effectively are unique skills improved with formal training and experience. To be sure, divergent thinking is often not appreciated in such hierarchical institutions as the armed forces and law enforcement.[152] "Your ability to mind read is more praiseworthy than your ability to think critically" according to a

[149] Zenko, *Red Team: How to Succeed by Thinking Like the Enemy*, 117.

[150] Ibid., 122.

[151] Ibid., 123.

[152] Ibid., 33.

United States Marine Corps red team officer quoted in Zenko's book, *Red Team*. Individuals might resist questioning the status quo out of fear of risking career advancement or simply because they are so ingrained in the corporate culture that they lack the ability to see outside the organizational framework. A poorly staffed red team may actually only further solidify agencies' organizational assumptions and provide false confidence in a plan not truly evaluated critically.

3. Red Team Independence

Third, the leadership of an operation must invite red team participants into each phase of the planning process and provide them with support to express ideas that might not be embraced throughout the organization.[153] This support is in the form of access to key decision makers, proper resources, personnel, and authority to complete the assessment.[154] The team must have independence from the main body that they are evaluating or risk being made subordinate to the overall organization.[155] Without independence, the red team process can be manipulated to support a predetermined desired result and become a rubber stamp on policies and programs. An example of this rubber stamp can be seen in the way President Lyndon B. Johnson used the devil's advocate technique during the Vietnam War to give the appearance of authentic debate. Under Secretary of State George Ball expressed dissent to the escalation of bombing in North Vietnam in senior-level meetings and his contrarian view was explained away by President Johnson as merely the result of his assuming the devil's advocate role.[156] Once Bell left his position in the State Department, President Johnson reassigned the devil's advocate role to senior aide Bill Moyers; however, this reassignment was merely to give the appearance of true debate.[157] According to Johnson's press secretary George Reedy, "objections and cautions are discounted before they are delivered. They are actually

[153] Defense Science Board, *The Role and Status of DoD Red Teaming Activities*, 6.

[154] Zenko, *Red Team: How to Succeed by Thinking Like the Enemy*, 4.

[155] Defense Science Board, *The Role and Status of DoD Red Teaming Activities*, 6.

[156] Zenko, *Red Team: How to Succeed by Thinking Like the Enemy*, 218–219.

[157] Ibid.

welcomed because they prove for the record that decision was preceded by controversy."[158]

Another example of the need for red team independence is the 2002 U.S. Joint Forces Command (JFCOM) war game *Millennium Challenge 02 (MC)*, highlighted in Malcom Gladwell's 2005 book, *Blink: The Power of Thinking without Thinking*. This unscripted exercise was designed to be a combination of advanced computer model simulation and actual troop and equipment movements in the field occurring in real-time and involving over 13,500 service members at a cost of $250 million.[159] The Pentagon designed this exercise in anticipation that the future of warfare would be less conventional and the nation's adversaries would recognize the futility of engaging the United States in direct military conflict.[160] The MC was designed to test the U.S. military's ability to wage war against a non-traditional threat. Secretary of Defense Donald Rumsfeld stated the goal of the MC was to "help us create a force that is not only interoperable, responsive, agile and lethal, but one that is capable of capitalizing on the information revolution and the advanced technologies that are available today."[161]

This exercise pitted the United States (Blue Team) against a fictitious rogue military commander somewhere in the Persian Gulf (Red Team) in the year 2007.[162] Blue Team commanders were provided with intelligence and almost every technological and military capability in the U.S. arsenal.[163] The simulation exercise began with the Blue Team issuing an eight-point ultimatum to the Red Team including a demand for full surrender.[164] Instead of diplomatically negotiating with the far superior military Blue

---

[158] George Reedy, *The Twilight of a Presidency* (Cleveland, OH: World Publishing Company, 1970), 11.

[159] Zenko, *Red Team: How to Succeed by Thinking Like the Enemy*, 52–53.

[160] Malcolm Gladwell, *Blink: The Power of Thinking without Thinking* (New York: Back Bay Books, 2005), 104.

[161] Jim Garamone, "Rumsfeld Visits Millennium Challenge Exercise," *American Forces Press Service*, July 29, 2002, http://www.globalsecurity.org/military/library/news/2002/07/mil-020729-dod01.htm.

[162] Although not specifically stated in formal planning documents, the Red Team was largely understood by exercise participants to represent Iraq or Iran.

[163] Gladwell, *Blink*, 105.

[164] Zenko, *Red Team: How to Succeed by Thinking Like the Enemy*, 55.

Team, the Red Team launched a preemptive attack on U.S. naval ships as soon as it entered the Persian Gulf. Within 10 minutes, the Red Team overwhelmed the Blue Navy and sank 19 ships using techniques far from modern. The Red Team used a combination of "a barrage of missiles from ground-based launchers, commercial ships, and planes flying low and without radio communications to reduce radar signature."[165] The opposing force also used speedboats packed with explosives to conduct suicide missions against the U.S. fleet with tremendous success.[166] The Blue Team cut all fiber optic and microwave communication capability in an attempt to force the Red Team to rely upon easily intercepted cellular and satellite communications.[167] The Red Team responded by switching their communications to couriers on motorcycles completely negating the Blue Team's technological advantage.[168] With the Red Team inflicting massive and unexpected damage on the Blue Team on the first day of the exercise, the overall commanders felt like they had no choice but to reset the simulation.

They began issuing orders to the Red Team limiting its operational capabilities, which, in turn, made its responses fully predictable to Blue Team commanders. The Red Team commander, a retired U.S. Marine Corps Lieutenant General, stepped down mid-simulation as the exercise became more scripted.[169]

At the conclusion of the exercise, the Blue Team achieved a convincing simulated victory, but not without controversy. The Red Team commander completed a report upon the conclusion of this simulation expressing concern that this exercise was "controlled and how the exercise could lead the Pentagon to have misplaced confidence in what were still-untested military war-fighting concepts."[170] This massive simulation was designed to test the American military's ability to fight in unconventional warfare; however, the lack of independence in the Red Team minimized the potential benefits of this exercise.

---

[165] Zenko, *Red Team: How to Succeed by Thinking Like the Enemy*, 56.

[166] Ibid.

[167] Gladwell, *Blink*, 109.

[168] Ibid.

[169] Zenko, *Red Team: How to Succeed by Thinking Like the Enemy*, 57.

[170] Ibid. Operation Iraqi Freedom began in March 2003.

C. CONCLUSION

Mark Mateski of *The Red Team Journal* states that an expert red team has the "ability to help expose a decision-maker's blinders, preconceptions, and biases."[171] These techniques have the potential to enhance the security planning for major events, but these improvements are only derived when conducted by trained individuals and for organizations open to having their plans and assumptions challenged. Red team execution traps and pitfalls have the potential to reduce the overall effectiveness of these techniques.

[171] Mateski, "Red Team: A Balanced View."

VI. FINDINGS, PROPOSALS, AND CONCLUSIONS

> Victory smiles upon those who anticipate the changes of war, not upon those who wait to adapt themselves after the change occurs.
>
> ~ Giulio Douhet—1922

The security planning for major events requires the participation of dozens of local, state, and federal law enforcement, fire, and life safety entities working in coordination. The subcommittee process employed in these major events has proven effective in marshaling tremendous amounts of resources and ensuring that areas of responsibility are well-defined; however, it leaves open the potential for individual and organizational biases to impact planning. The 2009 presidential inauguration case study demonstrated that even with significant amounts of time and resources, highly experienced planners still use mental shortcuts, or assumptions, to fill in missing information that can lead to poor outcomes.

The failure to anticipate the behavior of the event participants in the inauguration did not result in fatalities; however, it should be used as a cautionary tale for those individuals and organizations responsible for the safety and security of these major events. It is impossible to determine how often these types of planning errors have occurred in previous major events, but the results of this research indicate that a potential exists for recurrence within the subcommittee framework. The organizational structure of major-event security planning creates information "silos" within which individual and group decision-making errors can occur.

This thesis has investigated the need for and potential benefits of formally adopting a red team mechanism into the security subcommittee framework of major events. The capabilities of these red team techniques theoretically offer the potential to reduce poor planning and are designed to "challenge facts and explicit assumptions, look for implicit (unstated) assumptions, identify cultural assumptions and develop targeted cultural questions for subject matter experts, challenging the problem frame (and proposing alternative frames), identifying cognitive biases and symptoms of underlying

groupthink."[172] The execution of these techniques, however, can be challenging and diminish the effectiveness of red teaming.

These techniques are currently being used in both the DOD and the American IC and these organizations share many similarities with the law enforcement agencies that participate in the security design and execution for major event security. As such, the formal adoption of red team techniques within major event security appeared to be a natural fit. Research on red teams, however, indicates that their effectiveness varies on the organizational leadership, team training and composition, and independence afforded these teams in the performance of their assignment. The execution traps outlined in Chapter II indicate that these techniques can be difficult to implement successfully. Organizations experienced in "grading their own homework" may resist having their planning decisions exposed to outside review and criticism.[173] Additionally, red teams must be provided a degree of independence to question an organization's plans without fear of reprisal or simply being made a "rubber stamp" to a predetermined course of action, such as President Johnson's use of the devil's advocate during the Vietnam War. The formal adoption of red team techniques has the potential to improve decision making in major events; however, these events are not planned and executed in a vacuum. If not properly supported and implemented, attempts to red team major security planning may only solidify commonly accepted assumptions and paradoxically work against the goal of helping planners see situations, problems, and solutions from alternate perspectives.[174] The MC 02 exercise outlined in Chapter II demonstrated that red teaming can be manipulated to pervert the planning process.

A. RED TEAM PROPOSALS

The use of analytical red team techniques in major-event security planning has the potential to improve the overall process by reducing individual and group decision-making errors. This section advances two different proposals to inject red team

[172] University of Foreign Military and Cultural Studies, *The Applied Critical Thinking Handbook (formerly the Red Team Handbook)*, 3.

[173] Zenko, *Red Team: How to Succeed by Thinking Like the Enemy*, 3.

[174] United States Joint Force Development, *Command Red Team*, V.

techniques into major-event security planning for consideration. Each proposal has specific strengths and weaknesses that would need to be considered prior to implementation and are discussed in this section.

1. DHS Major Event Red Team Pilot Program

The DHS should design, staff, and implement its own red team composed of subject-matter experts selected from department component agencies. Volunteers would apply to the DHS to serve on a part-time red team whose purpose is to support the subcommittee model at NSSE and SEAR 1 events. Initially, the DHS should contract directly with the UFMCS, Fort Leavenworth, Kansas, to design a groupthink mitigation and analytic analysis program for these members. The UFMCS has a demonstrated ability to educate DOD officials in these techniques and would be considered the subject-matter experts in this area until the DHS can develop its own in-house capability.

This team would be activated to support NSSE and SEAR 1 executive and subcommittees and would provide an analysis of operational plans two months before the event date.[175] This timeline would enable the subcommittee in question to adjust resources and priorities if needed. This red team should also be involved in providing after-action reviews and post-event analysis to assist in determining if the final security plan contained poor assumptions or weaknesses available for exploitation. These "lessons learned" would then be captured for future use in the security planning for similar major events. This benefit would be especially useful for events that occur in the same location yearly, such as the United Nation's General Assembly in New York or the State of the Union Address held in Washington, DC.

A Major Event Red Team (MERT) pilot program would train current DHS subject-matter experts in red team techniques. This unified DHS team would share a common command structure and report directly to the executive committee, as well as the department itself. Access to the individual subcommittees and their plans would need to be ensured for the MERT to be of value. A senior-level team leader with experience in

[175] This two-month timeline would be waived for events with short planning cycles, such as presidential funerals.

major event planning should be selected by the department to protect against the red team becoming subordinate to the executive committee and also to increase the likelihood that the red team results are considered by the security subcommittees.[176]

The MERT program should last initially for 36 months. This period allows for a sufficient number of major events to occur for the program to be evaluated. Evaluation metrics for program consideration include adjustments made by the subcommittees based on MERT recommendations, feedback from subcommittee chairs, and after-action reviews of final event plans. The future development of a training curriculum within the DHS would depend on the initial pilot program results and funding. Additionally, this trained cadre of red team practitioners would remain within the DHS and could bring those skills back to their component agencies for an ancillary benefit to the department.

2. Executive and Subcommittee Chair Red Team Education

The DHS should contract with the UFMCS to design and implement a groupthink mitigation program and analytical analysis program exactly as in recommendation 1. This program should then be offered specifically to executive and subcommittee chairs at the local, state, and federal level prior to the initiation of NSSE and SEAR 1 planning. These chairs will be responsible to lead all subcommittee meetings within which poor planning can potentially occur and having them trained in analytical techniques at the onset may assist in reducing the potential incidents of groupthink early in the process. The potential benefits of this recommendation include red team trained individuals physically present during all phases of plan formulation, a greater likelihood of executive and subcommittee leadership acceptance of techniques, less cost to the DHS, as local and state chairs are responsible for their own expenses in attending the course, and less impact to the DHS component agencies as compared to recommendation 1.

This recommendation also has significant negatives that need to be carefully considered prior to implementation. First, individuals instrumental and emotionally close to planning often have a difficult time acknowledging shortcomings, which is one of the

[176] Defense Science Board, *The Role and Status of DoD Red Teaming Activities*, 6. The team leader should match the rank of the executive committee membership, which is traditionally a GS-15 or equivalent.

hallmarks of groupthink. This recommendation assumes that red team trained subcommittee chairs will bring back the lessons to their planning operations and put them to immediate use. The DOD has determined that not everyone is suited to serve in a red team capacity, and therefore, the results will likely be inconsistent as different planners will embrace these techniques at various levels.[177]

B. CONCLUSION

This thesis has explored the varieties of red team techniques available to major event security planners and asked the question: *How would the Department of Homeland Security (DHS) benefit from formally adopting a red team component to major-event security planning?* The potential benefits and drawbacks of simulations, vulnerability probes, and analytical techniques have also been explored in this project. Based on the findings on red team performance and execution pitfalls, this thesis has made two proposals to insert an analytical red team capability formally into the framework used in major-event security planning. The proposals have the potential to place properly trained individuals into the framework at the appropriate time to make improvements into the planning process. These proposals, however, will have to navigate the minefield of potential execution errors outlined in this thesis. While the DHS theoretically will benefit from the formal adoption of analytical red team techniques, the execution limitations discussed in this thesis reduce the likelihood for ideal results. The DHS needs to consider these limitations before formally adopting a red team component into the framework for major-event security planning.

[177] Defense Science Board, *The Role and Status of DoD Red Teaming Activities*, 7.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Abcarian, Robin. “They Came for the Inauguration but Got Stuck in a Tunnel.” *The Los Angeles Times*, January 23, 2009. http://articles.latimes.com/2009/jan/23/nation/na-angry-inauguration-goers23.

Aldag, Ramon, and Sally Riggs Fuller. “Beyond Fiascos: A Reappraisal of the Groupthink Phenomenon and a New Model of Group Decision Processes.” *The Psychological Bulletin* 113, no. 3 (1993): 533–552.

Associated Press, The. “Feds Say Inauguration an Attractive Terrorist Target.” *NBC News*, January 7, 2009. http://www.nbcnews.com/id/28547871/ns/politics-inauguration/t/feds-say-inauguration-attractive-terrorist-target/#.V_k1wsZFDIU.

Bennett, Brian. “Red Team Agents Use Disguises, Ingenuity to Expose TSA Vulnerabilities.” *Los Angeles Times*, June 2, 2015. http://www.latimes.com/nation/nationnow/.

Chen, Zenglo, Robert Lawson, Lawrence Gordon, and Barbara McIntonsh. “Groupthink: Deciding with the Leader and Devil.” *The Psychological Record* 46, no. 4 (Fall 1996). http://www.thefreelibrary.com/Groupthink%3a+deciding+with+the+leader+and+the+devil.-a018911798.

Chu, Vivian, and Tammy Felix. *Command, Control, and Coordination: A Quick-Look Analysis of the Charlotte-Mecklenberg Police Department’s Operations During the 2012 Democratic National Convention.* (IQR-2013-U-004229). Washington, DC: Department of Justice, Bureau of Justice Assistance and Alexandria, VA: CNA Analysis & Solutions, 2013. https://www.bja.gov/Publications/2012-DNC-Quick-Look.pdf.

CNN. “Official Inauguration Crowd Estimate: 1.8 Million.” January 22, 2009. http://politicalticker.blogs.cnn.com/2009/01/22/official-inauguration-crowd-estimate-18-million/.

Constable, Pamela, and Mary Beth Sheridan. “And Then We Knew It Was Too Late.” *Washington Post*, January 21, 2009. http://www.washingtonpost.com/wp-dyn/content/article/2009/01/20/AR2009012003362.html.

Dattner, Ben. “Preventing “Groupthink”.” *Psychology Today*, April 20, 2011. https://www.psychologytoday.com/blog/credit-and-blame-work/201104/preventing-groupthink.

Davis, Mark. “How 9/11 Affected the U.S. Stock Market.” Investopedia, September 9, 2011. http://www.investopedia.com/financial-edge/0911/how-september-11-affected-the-u.s.-stock-market.aspx.

Dean, Matthew. “Secret Service Training in High Gear Ahead of Inauguration Day.” *Fox News*, January 13, 2017. http://www.foxnews.com/politics/2017/01/13/secret-service-training-in-high-gear-ahead-inauguration-day.html.

Defense Science Board. *The Role and Status of DoD Red Teaming Activities*. Washington, DC: Office of the Under Secretary of Defense, 2003.

Department of Defense. “Statement by Pentagon Press Secretary Peter Cook on DoD’s “Hack the Pentagon” Cybersecurity Initiative.” Release No: NR-070-16, March 2, 2016. http://www.defense.gov/News/News-Releases/News-Release-View/Article/684106/statement-by-pentagon-press-secretary-peter-cook-on-dods-hack-the-pentagon-cybe.

Department of Homeland Security. *Homeland Security Protection Directive 5—Management of Domestic Incidents*. Washington, DC: Department of Homeland Security, 2003. https://www.dhs.gov/sites/default/files/publications/Homeland%20Security%20Presidential%20Directive%205.pdf.

Dorner, Dietrich. *The Logic of Failure*. New York: Metropolitan Book, 1996.

Fontenot, Gregory. “Seeing Red: Creating a Red-Team Capability for the Blue Force.” *Military Review*, September–October 2005.

Garamone, Jim. “Rumsfeld Visits Millennium Challenge Exercise.” *American Forces Press Service*, July 29, 2002. http://www.globalsecurity.org/military/library/news/2002/07/mil-020729-dod01.htm.

Garratt, R. Sam, and Shawn Reese. *Funding of Presidential Nominating Conventions: An Overview*. (CRS Report No R46937). Washington, DC: Congressional Research Service, 2016. https://fas.org/sgp/crs/misc/R43976.pdf.

Gehring, James. “Sports Venue Security: Public Policy Options for SEAR 4–5 Events.” Master’s thesis, Naval Postgraduate School, 2014.

Gillian, Tet. *The Silo Effect*. New York: Simon and Schuster, 2015.

Gladwell, Malcolm. *Blink: The Power of Thinking without Thinking*. New York: Back Bay Books, 2005.

Goodman, J. David. “Pope’s Visit Poses a Security Test for New York.” *The New York Times*, September 14, 2015. http://www.nytimes.com/2015/09/15/nyregion/pope-francis-visit-prompts-security-preparations-in-new-york.html?_r=0.

Hood, M. Brent. “Us versus Them: Effects of Group Dynamics on Leadership.” FBI Law Enforcement Bulletin, June 2015. https://leb.fbi.gov/2015/june/us-versus-them-effects-of-group-dynamics-on-leadership.

Janis, Irving. *Groupthink: Psychological Studies of Policy Decisions and Fiascos.* Boston: Houston Mifflin Company, 1982.

Joint Congressional Committee on Inaugural Ceremonies. *JCCIC Releases Map and Ticket Information for Inaugural Swearing-In Ceremonies*. Washington, DC: Joint Congressional Committee on Inaugural Ceremonies, 2009. http://www.wmata.com/getting_around/metro_events/ticket-map_release.pdf.

Kahneman, Daniel. *Thinking, Fast and Slow*. New York: Farrar, Straus, and Giroux, 2011.

Kam, Ephraim. *Surprise Attack: A Victim's Perspective*. Cambridge, MA: Harvard University Press, 1988.

Klein, Gary. *Seeing What Others Don't*. New York: Public Affairs Press, 2013.

Kornreich, Lauren. "Arrive Early, Wear Comfy Shoes on Inauguration Day." *CNN*, January 19, 2009. http://www.cnn.com/2009/TRAVEL/01/18/inauguration.travel/index.html.

Lantz, Megan. Facebook post. "Survivors of the Purple Tunnel of Doom." January 21, 2009. https://www.facebook.com/groups/61444130820/.

Linkins, Jason. "Purple Ticket Turmoil Explained: What Happened on Inauguration Day." *The Huffington Post*, updated May 25, 2011. http://www.huffingtonpost.com/2009/01/23/purple-ticket-turmoil-wha_n_160150.html.

Mateski, Mark. "Red Teaming: A Balanced View." *The Red Team Journal*, February 14, 2013. http://redteamjournal.com/2013/02/red-teaming-a-balanced-view/.

Max, Shelley. Facebook post. "Survivors of the Purple Tunnel of Doom." January 22, 2009. https://www.facebook.com/groups/61444130820/.

Mueller, Jennifer S., Shimul Melwani, and Jack A. Goncalo. "The Bias Against Creativity: Why People Desire but Reject Creative Ideas." *Psychological Science* 23, no. 1 (2012): 1–20.

Nakamura, David. "Sen. Feinstein Launches Investigation into Ticket Fiasco." *Washington Post*, January 21, 2009. http://voices.washingtonpost.com/inauguration-watch/2009/01/sen_feinstein_launches_investi.html.

Nicole, Kristin. "Purple Tunnel of Doom Gets Authority's Attention." *Social Times*, January 27, 2009. http://www.adweek.com/socialtimes/purple-tunnel-doom-facebook-group/306741.

North American Aerospace Command. “NORAD Exercise Planned for Super Bowl XILX.” January 26, 2015. http://www.norad.mil/Newsroom/Press-Releases/Article/578766/norad-exercise-planned-for-super-bowl-xlix/.

Reedy, George. *The Twilight of a Presidency*. Cleveland, OH: World Publishing Company, 1970.

Ricciuti, James E. “Groupthink: A Significant Threat to the Homeland Security of the United States.” Master’s thesis, Naval Postgraduate School, 2014.

Rodriguez-King, Denise, and Tammy Felix. *Command, Control, and Coordination: A Quick-Look Analysis of the Tampa Police Department’s Operations During the 2012 Republican National Convention*. (IQR-2013-U-004228). Washington, DC: Department of Justice, Bureau of Justice Assistance and Alexandria, VA: CNA Analysis & Solutions, 2013. https://www.bja.gov/Publications/2012-RNC-Quick-Look.pdf.

Rozen, Laura. “Purple Tunnel of Doom After-action Report: “Survivors” Offer Lessons Learned.” *Foreign Policy*, January 21, 2009. http://foreignpolicy.com/2009/01/21/purple-tunnel-of-doom-after-action-report-survivors-offer-lessons-learned/.

Ruane, Michael E., and Nikita Stewart. “Practice Inauguration Lacks Some Pomp and the VIPs.” *The Washington Post*, January 12, 2009. http://www.washingtonpost.com/wp-dyn/content/article/2009/01/11/AR2009011100625.html?sid=ST2009011102548.

Scott, Esther. *Security Planning for the 2004 Democratic National Convention (B)*. Cambridge, MA: Kennedy School of Government, 2005.

Sheridan, Mary Beth, and Pamela Constable. “Inaugural Missteps and Miscalculations.” *Washington Post*, January 25, 2009. http://www.washingtonpost.com/wp-dyn/content/article/2009/01/24/AR2009012401928.html.

Sunstein, Cass, and Reid Hastie. *Wiser: Getting Beyond Groupthink to Make Groups Smarter*. Boston: Harvard Business Review Press, 2015.

Tavris, Carol, and Elliot Aronson. *Mistakes Were Made (but Not by Me).* New York: Houghton Mifflin, 2015.

Tversky, Amos, and Daniel Kahneman. “Judgment under Uncertainty: Heuristics and Biases.” *Science* 185, no. 4157 (September 27, 1974): 1124–1131.

United States Joint Force Development. *Command Red Team*. (Joint Doctrine Note 1–16). Washington, DC: United States Joint Force Development, 2016. http://dtic.mil/doctrine/notes/jdn1_16.pdf.

United States Secret Service. *Multi-Agency Response to Concerns Raised by the Joint Congressional Committee on the Inaugural Ceremonies for the 56th Presidential Inauguration*. Washington, DC: United States Secret Service, 2009.

University of Foreign Military and Cultural Studies. *The Applied Critical Thinking Handbook (formerly the Red Team Handbook)*. ver. 8.1. Fort Leavenworth, KS: University of Foreign Military and Cultural Studies, 2016.

Washington Metropolitan Area Transit Authority. "Metro Outlines Inauguration Day Service Plans." Accessed December 22, 2016. http://www.wmata.com/about_metro/news/PressReleaseDetail.cfm?ReleaseID=2424.

White House, The. *Presidential Decision Directive NSC/62*. Washington, DC: The White House, 1998. http://fas.org/irp/offdocs/pdd/pdd-62.pdf.

Willbrich, Sara. Facebook post. "Survivors of the Purple Tunnel of Doom." January 22, 2009. https://www.facebook.com/groups/61444130820/.

Zenko, Micah. *Red Team: How to Succeed by Thinking Like the Enemy*. New York: Basic Books, 2015.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California